Konfigurieren von Windows 7 – Original Microsoft Training für Examen 70-680

Microsoft Press

Dieses Buch ist die deutsche Übersetzung von: Ian McLean, Orin Thomas:
MCTS Self-Paced Training Kit (Exam 70-680): Configuring Windows 7
Microsoft Press, Redmond, Washington 98052-6399
Copyright 2010 Microsoft Corporation

Das in diesem Buch enthaltene Programmmaterial ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor, Übersetzer und der Verlag übernehmen folglich keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programmmaterials oder Teilen davon entsteht.

Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen sowie E-Mail-Adressen und Logos sind frei erfunden, soweit nichts anderes angegeben ist. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen, E-Mail-Adressen und Logos ist rein zufällig.

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
12 11 10

ISBN 978-3-86645-980-9

© Microsoft Press Deutschland
(ein Unternehmensbereich der Microsoft Deutschland GmbH)
Konrad-Zuse-Str. 1, D-85716 Unterschleißheim
Alle Rechte vorbehalten

Übersetzung: Detlef Johannis, Kempten, Michael Ringel, Bonn
Korrektorat: Claudia Mantel-Rehbach, Entraching
Fachlektorat und Satz: Günter Jürgensmeier, München
Umschlaggestaltung: Hommer Design GmbH, Haar (www.HommerDesign.com)
Layout und Gesamtherstellung: Kösel, Krugzell (www.KoeselBuch.de)

Inhaltsverzeichnis

Danksagungen . . . . . **XV**
Einführung . . . . . **XVII**
Einrichten der Testumgebung XVIII
Hardwarevoraussetzungen XVIII
Softwarevoraussetzungen XIX
Verwenden der Begleit-CD XIX
So installieren Sie die Übungstests XX
So benutzen Sie die Übungstests XX
So deinstallieren Sie die Übungstests XXI
Das Microsoft Certified Professional-Programm XXI
Support XXII

Kapitel 1: Installieren, Migrieren oder Aktualisieren auf Windows 7 . . . . . **1**
Bevor Sie beginnen 2
Lektion 1: Installieren von Windows 7 3
Windows 7-Editionen 3
Hardwarevoraussetzungen für Windows 7 5
Vorbereiten der Windows 7-Installationsquelle 6
Installieren von Windows 7 9
Zusammenfassung der Lektion 22
Lernzielkontrolle 23
Lektion 2: Aktualisieren auf Windows 7 25
Aktualisieren von Windows 7-Editionen 25
Aktualisieren von Windows Vista 26
Migrieren von Windows XP 29
Zusammenfassung der Lektion 32
Lernzielkontrolle 32
Lektion 3: Verwalten von Benutzerprofilen 34
Migrieren von Benutzerprofildaten 34
Windows-EasyTransfer 35
User State Migration Tool 39
Zusammenfassung der Lektion 46
Lernzielkontrolle 46
Rückblick auf dieses Kapitel 48
Zusammenfassung des Kapitels 48
Schlüsselbegriffe 49
Übungen mit Fallbeispiel 49
Übung 1: Installieren von Windows 7 bei Contoso 49
Übung 2: Migrieren von Benutzerdaten bei Fabrikam 49

Vorgeschlagene Übungen 50
Durchführen einer Neuinstallation 50
Aktualisieren einer älteren Windows-Version auf Windows 7 50
Migrieren der Benutzerprofile 50
Machen Sie einen Übungstest 51

Kapitel 2: Konfigurieren von Systemabbildern 53
Bevor Sie beginnen 54
Lektion 1: Aufzeichnen von Systemabbildern 55
Installieren und Benutzen des Windows Automated Installation Toolkit 55
Arbeiten mit Windows PE 57
Erstellen eines Referenzabbilds 58
Verteilen eines Abbilds auf viele Computer 71
Verwenden von DISM 74
Vorbereiten einer Windows 7-Installation mit Sysprep 76
Zusammenfassung der Lektion 85
Lernzielkontrolle 86
Lektion 2: Verwalten von virtuellen Festplatten 88
Verwenden nativer VHDs in Windows 7 88
Verwenden des Tools WIM2VHD 93
Aktualisieren einer VHD mit dem Offline Virtual Machine Servicing Tool 95
Bereitstellen in einer Online-VHD mithilfe der Windows-Bereitstellungsdienste 96
Zusammenfassung der Lektion 107
Lernzielkontrolle 107
Rückblick auf dieses Kapitel 109
Zusammenfassung des Kapitels 109
Schlüsselbegriffe 109
Übungen mit Fallbeispiel 110
Übung mit Fallbeispiel 1: Generieren eines Systemabbilds 110
Übung mit Fallbeispiel 2: Arbeiten mit VHDs 110
Vorgeschlagene Übungen 111
Verwenden von Windows SIM und Sysprep 111
Arbeiten mit VHDs 111
Machen Sie einen Übungstest 112

Kapitel 3: Bereitstellen von Systemabbildern 113
Bevor Sie beginnen 114
Lektion 1: Verwalten eines Systemabbilds vor der Bereitstellung 115
Verwenden der WIM-Befehle von DISM und Bereitstellen eines Abbilds im Dateisystem 116
Warten von Treibern, Anwendungen, Patches, Paketen und Features 122
Warten von Windows PE-Abbildern 133
Befehlszeilenoptionen für unbeaufsichtigte Bearbeitung 135
Zusammenfassung der Lektion 142
Lernzielkontrolle 142

Lektion 2: Bereitstellen von Abbildern 144
Arbeiten mit dem Microsoft Deployment Toolkit 144
Verwalten und Verteilen von Abbildern mit MDT 2010 149
Bereitstellen von Abbildern mit WDS 165
Verwenden von SCCM 2007 172
Ein Abbild von Hand installieren 177
Zusammenfassung der Lektion 184
Lernzielkontrolle 184
Rückblick auf dieses Kapitel 186
Zusammenfassung des Kapitels 186
Schlüsselbegriffe 186
Übungen mit Fallbeispiel 187
Übung mit Fallbeispiel 1: Bereitstellen eines Abbilds mit mehreren Language Packs . . 187
Übung mit Fallbeispiel 2: Bereitstellen eines Abbilds auf 100 Clientcomputern 187
Vorgeschlagene Übungen 188
Verwalten und Bearbeiten eines Systemabbilds 188
Machen Sie sich mit den Bereitstellungstools vertraut 188
Machen Sie einen Übungstest 189

Kapitel 4: Verwalten von Geräten und Datenträgern 191
Bevor Sie beginnen 192
Lektion 1: Verwalten von Gerätetreibern und Geräten 193
Anzeigen von Geräteinformationen im Geräte-Manager 193
Installieren von Geräten und Verwalten von Gerätetreibern 199
Zusammenfassung der Lektion 222
Lernzielkontrolle 223
Lektion 2: Verwalten von Datenträgern 225
Datenträgerwartung 225
Ändern von Datenträgertyp und Partitionsstil 232
Verwalten von Datenträgervolumes 239
Zusammenfassung der Lektion 248
Lernzielkontrolle 248
Rückblick auf dieses Kapitel 250
Zusammenfassung des Kapitels 250
Schlüsselbegriffe 250
Übungen mit Fallbeispiel 251
Übung mit Fallbeispiel 1: Erzwingen einer Treibersignierungsrichtlinie 251
Übung mit Fallbeispiel 2: Verwalten von Datenträgern 251
Vorgeschlagene Übungen 252
Untersuchen der Gruppenrichtlinien, die für die Verwaltung der Geräteinstallation zur Verfügung stehen 252
Arbeiten mit dem Treiberüberprüfungs-Manager 252
Verwenden von Diskpart 252
Machen Sie einen Übungstest 252

Kapitel 5: Verwalten von Anwendungen **253**
Bevor Sie beginnen 254
Lektion 1: Anwendungskompatibilität 255
Konfigurieren der Kompatibilitätsoptionen 255
Das Application Compatibility Toolkit 258
Richtlinien zur Anwendungskompatibilitätsdiagnose 262
Windows XP Mode für Windows 7 263
Zusammenfassung der Lektion 266
Lernzielkontrolle 267
Lektion 2: Verwalten von AppLocker und der Richtlinien für Softwareeinschränkung 269
Richtlinien für Softwareeinschränkung 269
AppLocker-Anwendungssteuerungsrichtlinien 275
Zusammenfassung der Lektion 288
Lernzielkontrolle 289
Rückblick auf dieses Kapitel 291
Zusammenfassung des Kapitels 291
Schlüsselbegriffe 292
Übungen mit Fallbeispiel 292
Übung 1: Konfigurieren der Anwendungskompatibilität bei Fabrikam 292
Übung 2: Beschränken von Anwendungen bei Contoso 292
Vorgeschlagene Übungen 293
Konfigurieren der Anwendungskompatibilität 293
Konfigurieren von Anwendungseinschränkungen 293
Machen Sie einen Übungstest 294

Kapitel 6: Netzwerkeinstellungen **295**
Bevor Sie beginnen 296
Lektion 1: Konfigurieren von IPv4 297
Grundlagen von IPv4-Adressen 298
Herstellen der Verbindung zu einem Netzwerk 305
Beseitigen von Netzwerkproblemen 308
Zusammenfassung der Lektion 323
Lernzielkontrolle 324
Lektion 2: Konfigurieren von IPv6 326
Aufbau von IPv6-Adressen 326
Die Vorteile von IPv6 331
Implementieren von IPv4-zu-IPv6-Kompatibilität 332
Konfigurieren von IPv6-Verbindungen 336
Zusammenfassung der Lektion 343
Lernzielkontrolle 343
Lektion 3: Netzwerkkonfiguration 345
Herstellen der Verbindung zu einem Netzwerk 345
Verwalten von Netzwerkverbindungen 360
Problembehandlung für Drahtlosnetzwerke 361
Konfigurieren der Sicherheit für Drahtlosnetzwerke 365
Verbesserungen beim Drucken in Windows 7 367
Zusammenfassung der Lektion 372
Lernzielkontrolle 372

Rückblick auf dieses Kapitel . . . 375
Zusammenfassung des Kapitels . . . 375
Schlüsselbegriffe . . . 375
Übungen mit Fallbeispiel . . . 376
Übung mit Fallbeispiel 1: Implementieren der IPv4-Konnektivität . . . 376
Übung mit Fallbeispiel 2: Implementieren der IPv6-Konnektivität . . . 376
Übung mit Fallbeispiel 3: Verwenden von Windows 7-Notebooks in Drahtlosnetzwerken . . . 376
Vorgeschlagene Übungen . . . 377
Konfigurieren von IPv4 . . . 377
Konfigurieren von IPv6 . . . 377
Konfigurieren von Netzwerken . . . 378
Machen Sie einen Übungstest . . . 378

Kapitel 7: Windows-Firewall und Remoteverwaltung . . . 379
Bevor Sie beginnen . . . 380
Lektion 1: Verwalten der Windows-Firewall . . . 381
Windows-Firewall . . . 381
Die Windows-Firewall mit erweiterter Sicherheit . . . 387
Zusammenfassung der Lektion . . . 398
Lernzielkontrolle . . . 398
Lektion 2: Windows 7-Remoteverwaltung . . . 400
Remotedesktop . . . 400
Remoteunterstützung . . . 403
Windows-Remoteverwaltungsdienst . . . 406
Zusammenfassung der Lektion . . . 413
Lernzielkontrolle . . . 413
Rückblick auf dieses Kapitel . . . 415
Zusammenfassung des Kapitels . . . 415
Schlüsselbegriffe . . . 415
Übungen mit Fallbeispiel . . . 416
Übung 1: Client-Firewalls an einer Universität . . . 416
Übung 2: Desktopunterstützung in der Antarktis . . . 416
Vorgeschlagene Übungen . . . 417
Die Windows-Firewall konfigurieren . . . 417
Konfigurieren der Remoteverwaltung . . . 417
Machen Sie einen Übungstest . . . 417

Kapitel 8: BranchCache und Ressourcenfreigabe . . . 419
Bevor Sie beginnen . . . 420
Lektion 1: Freigeben von Ressourcen . . . 421
Netzwerk- und Freigabecenter . . . 421
Heimnetzgruppen . . . 423
Freigegebene Ordner . . . 425
Bibliotheken . . . 430
Freigeben von Druckern . . . 431
Zusammenfassung der Lektion . . . 438
Lernzielkontrolle . . . 438

Lektion 2: Ordner- und Dateizugriff 440
Datei- und Ordnerberechtigungen 440
Konfigurieren der Überwachung 447
Verschlüsselndes Dateisystem 449
Zusammenfassung der Lektion 457
Lernzielkontrolle 457
Lektion 3: Verwalten von BranchCache 459
BranchCache-Konzepte 459
Gehosteter Cache 460
Modus »Verteilter Cache« 460
Konfigurieren der Windows 7-BranchCache-Clients 461
Konfigurieren von Datei- und Webservern unter Windows Server 2008 R2 466
Zusammenfassung der Lektion 469
Lernzielkontrolle 469
Rückblick auf dieses Kapitel 471
Zusammenfassung des Kapitels 471
Schlüsselbegriffe 471
Übungen mit Fallbeispiel 472
Übung 1: Berechtigungen und Verschlüsselung 472
Übung 2: Konfigurieren der Contoso-Zweigstellen 472
Vorgeschlagene Übungen 473
Konfigurieren von freigegebenen Ressourcen 473
Konfigurieren des Datei- und Ordnerzugangs 473
Konfigurieren von BranchCache 473
Machen Sie einen Übungstest 473

Kapitel 9: Authentifizierung und Benutzerkontensteuerung 475
Bevor Sie beginnen 476
Lektion 1: Verwalten der Benutzerkontensteuerung 477
Benutzerkontensteuerung 477
Einstellungen der Benutzerkontensteuerung 478
Richtlinien für die Benutzerkontensteuerung 480
Secpol und die Konsole *Lokale Sicherheitsrichtlinie* 486
Zusammenfassung der Lektion 490
Lernzielkontrolle 490
Lektion 2: Windows 7-Authentifizierung und -autorisierung 493
Anmeldeinformationsverwaltung 493
Ausführen von Programmen als anderer Benutzer mit Runas 495
Konfigurieren von Benutzerrechten 496
Smartcards 498
Kontorichtlinien 499
Beheben von Authentifizierungsproblemen 500
Verwalten von Zertifikaten 502
Zusammenfassung der Lektion 508
Lernzielkontrolle 508
Rückblick auf dieses Kapitel 510
Zusammenfassung des Kapitels 510

Schlüsselbegriffe . . . 511
Übungen mit Fallbeispiel . . . 511
Übung 1: Benutzerkontensteuerung bei Coho Vineyard . . . 511
Übung 2: Beheben von Kennwortproblemen bei Wingtip Toys . . . 511
Vorgeschlagene Übungen . . . 512
Konfigurieren der Benutzerkontensteuerung . . . 512
Konfigurieren der Authentifizierung und Autorisierung . . . 512
Machen Sie einen Übungstest . . . 512

Kapitel 10: DirectAccess und VPN-Verbindungen . . . 513
Bevor Sie beginnen . . . 514
Lektion 1: Verwalten von DirectAccess . . . 515
Grundlagen von DirectAccess . . . 515
Der DirectAccess-Verbindungsaufbau . . . 516
Konfigurieren des DirectAccess-Clients . . . 517
Konfigurieren des DirectAccess-Servers . . . 521
Zusammenfassung der Lektion . . . 527
Lernzielkontrolle . . . 527
Lektion 2: Remoteverbindungen . . . 530
Virtuelle private Netzwerke . . . 530
VPN-Authentifizierungsprotokolle . . . 533
VPN-Reconnect . . . 535
NAP-Wartung . . . 536
Remotedesktop und die Veröffentlichung von Anwendungen . . . 537
Einwählverbindungen . . . 540
Konfigurieren von Windows 7 für die Annahme von eingehenden Verbindungen . . . 542
Überwachung von Remoteverbindungen . . . 544
Zusammenfassung der Lektion . . . 548
Lernzielkontrolle . . . 548
Rückblick auf dieses Kapitel . . . 550
Zusammenfassung des Kapitels . . . 550
Schlüsselbegriffe . . . 550
Übungen mit Fallbeispiel . . . 551
Übung 1: DirectAccess bei Wingtip Toys . . . 551
Übung 2: Remote Access bei Tailspin Toys . . . 551
Vorgeschlagene Übungen . . . 552
Konfigurieren von DirectAccess . . . 552
Konfigurieren von Remoteverbindungen . . . 552
Machen Sie einen Übungstest . . . 552

Kapitel 11: BitLocker und Mobilitätsoptionen . . . 553
Bevor Sie beginnen . . . 554
Lektion 1: Verwalten von BitLocker . . . 555
BitLocker . . . 555
BitLocker To Go . . . 564
Zusammenfassung der Lektion . . . 572
Lernzielkontrolle . . . 572

Lektion 2: Windows 7 und Mobilität . . . 574
Offlinedateien . . . 574
Energieoptionen unter Windows 7 . . . 582
Zusammenfassung der Lektion . . . 592
Lernzielkontrolle . . . 593
Rückblick auf dieses Kapitel . . . 595
Zusammenfassung des Kapitels . . . 595
Schlüsselbegriffe . . . 595
Übungen mit Fallbeispiel . . . 596
Übung 1: Zugriff auf Offlinedateien bei Contoso . . . 596
Übung 2: Verwenden von BitLocker bei Tailspin Toys . . . 596
Vorgeschlagene Übungen . . . 597
Konfigurieren von BitLocker und BitLocker To Go . . . 597
Konfigurieren der Mobilitätsoptionen . . . 597
Machen Sie einen Übungstest . . . 598

Kapitel 12: Windows Update und Windows Internet Explorer . . . 599
Bevor Sie beginnen . . . 600
Lektion 1: Aktualisieren von Windows 7 . . . 601
Konfigurieren von Windows Update . . . 601
Wartungscenter . . . 609
Windows Server Update Services . . . 610
Richtlinien für Windows Update . . . 613
Microsoft Baseline Security Analyzer . . . 617
Zusammenfassung der Lektion . . . 620
Lernzielkontrolle . . . 621
Lektion 2: Konfigurieren von Internet Explorer . . . 623
Die Kompatibilitätsansicht im Internet Explorer . . . 623
Konfigurieren von Sicherheitseinstellungen . . . 624
SmartScreen-Filter . . . 628
Verwalten des InPrivate-Modus . . . 628
Add-Ons und Suchanbieter . . . 631
Popupblocker . . . 633
Konfigurieren von SSL-Zertifikaten . . . 634
Zusammenfassung der Lektion . . . 642
Lernzielkontrolle . . . 642
Rückblick auf dieses Kapitel . . . 645
Zusammenfassung des Kapitels . . . 645
Schlüsselbegriffe . . . 645
Übungen mit Fallbeispiel . . . 646
Übung mit Fallbeispiel 1: Windows Update bei Contoso . . . 646
Übung mit Fallbeispiel 2: Internet Explorer bei Wingtip Toys . . . 646
Vorgeschlagene Übungen . . . 647
Konfigurieren von Updates für Windows 7 . . . 647
Konfigurieren von Internet Explorer . . . 647
Machen Sie einen Übungstest . . . 648

Kapitel 13: Überwachung und Leistung **649**
Bevor Sie beginnen 650
Lektion 1: Überwachen von Systemen 651
Systemüberwachung und Berichterstellung 651
Verfolgen von Zuverlässigkeit, Stabilität und Gesamtleistung des Systems 661
Arbeiten mit dem Wartungscenter 663
Systemprogramme zum Untersuchen von Prozessen und Diensten 666
Protokollieren und Weiterleiten von Ereignissen und Ereignisabonnements 676
Zusammenfassung der Lektion 690
Lernzielkontrolle 691
Lektion 2: Konfigurieren von Leistungseinstellungen 693
Abrufen von Systeminformationen mit WMI 693
Verwenden des Tools *Systemkonfiguration* 709
Verwenden der Konsole *Dienste* 711
Konfigurieren von Leistungsoptionen 713
Konfigurieren des Schreibcaches für Festplatten 715
Untersuchen von Leistungsproblemen mit der Ereignisanzeige 717
Konfigurieren von Prozessen im Task-Manager 718
Konfigurieren der Netzwerkleistung 719
Windows-Leistungsanalysetools 721
Zusammenfassung der Lektion 727
Lernzielkontrolle 727
Rückblick auf dieses Kapitel 729
Zusammenfassung des Kapitels 729
Schlüsselbegriffe 729
Übungen mit Fallbeispiel 730
Übung mit Fallbeispiel 1: Verwenden von Sammlungssätzen und Ereignisweiterleitung 730
Übung mit Fallbeispiel 2: Problembehandlung für Leistungsprobleme auf einem Clientcomputer 730
Vorgeschlagene Übungen 731
Arbeiten mit den Leistungsüberwachungstools 731
Verwalten der Ereignisprotokollierung 731
Schreiben von WMI-Skripts 731
Machen Sie einen Übungstest 732

Kapitel 14: Datensicherung und Wiederherstellung **733**
Bevor Sie beginnen 734
Lektion 1: Datensicherung 735
Planen von Datensicherungen in der Konsole *Sichern und Wiederherstellen* 735
Durchführen von Systemabbildsicherungen 743
Zusammenfassung der Lektion 748
Lernzielkontrolle 748
Lektion 2: Systemwiederherstellung 751
Durchführen einer Systemwiederherstellung 751
Erweiterte Startoptionen und Systemwiederherstellungsoptionen 756
Systemstartoptionen in Windows 7 759

Wiederherstellen der Vorversion eines Treibers 761
Zusammenfassung der Lektion 766
Lernzielkontrolle 766
Lektion 3: Wiederherstellen von Dateien und Ordnern 768
Wiederherstellen beschädigter oder gelöschter Dateien aus der Vorgängerversion 768
Konfigurieren von Computerschutz und Datenträgernutzung 776
Zusammenfassung der Lektion 781
Lernzielkontrolle 781
Zusammenfassung des Kapitels 784
Rückblick auf dieses Kapitel 784
Schlüsselbegriffe 784
Übungen mit Fallbeispiel 785
Übung mit Fallbeispiel 1: Support für Datensicherung und Wiederherstellung 785
Übung mit Fallbeispiel 2: Beseitigen von System- und Konfigurationsproblemen 785
Vorgeschlagene Übungen 786
Durchführen von Datensicherungen 786
Konfigurieren der Systemwiederherstellung 786
Wiederherstellen von Dateien und Ordnern 787
Machen Sie einen Übungstest 787

Antworten 789
Glossar 855
Stichwortverzeichnis 859
Die Autoren 885

Es ist ungewöhnlich, ein Buch einem seiner Autoren zu widmen, aber als sich Orin Thomas dazu bereiterklärte, mit mir zusammen Bücher zu schreiben, war dies mein Glückstag. Orin ist einer der kompetentesten und fähigsten IT-Experten, die mir je begegnet sind. Er weiß nicht nur, wie etwas gemacht wird, sondern kann dies auch noch verständlich erklären. Er ist mein wichtigster Fachlektor und mein Koautor. Seine fachlichen Kritiken sind ebenso gnadenlos wie informativ. Für beides werde ich ihm ewig dankbar sein. Er ist immer bereit einzuspringen, wenn ich irgendwelche Probleme habe. Lieber Orin – hör bloß nicht auf, meine Texte in der Luft zu zerreißen. Übrigens werde ich dasselbe für Dich tun, sollte ich die Gelegenheit dazu erhalten. Ich liebe es, mit einem echten Profi zusammenzuarbeiten.

IAN MCLEAN

Allen, die sich auf die Zertifizierungsreise begeben, wünsche ich, dass diese Reise ebenso lohnend wie nützlich wird und ebenso spannend, wie meine eigene Reise war. Viel Glück bei der Windows 7-Prüfung!

ORIN THOMAS

Danksagungen

Ein Buch zu schreiben ist immer Teamarbeit, und wir genießen den Vorteil, dass hinter der Bühne ein ausgezeichnetes Team für uns arbeitet. Im Gegensatz zu den Autoren sieht es aber die eigenen Namen niemals auf der Titelseite des Buchs. Wir möchten uns bei Kenn Jones bedanken, unserem Acquisitions Editor, der immer wieder sein Vertrauen in uns setzt, wenn es um ein neues Projekt geht, bei Laura Sackerman, unserem Developmental Editor, die uns in den ersten Phasen begleitet und bei Problemen zur Seite steht, wenn wir beispielsweise neue Vorlagen verwenden müssen, und bei Heather Stafford, deren Aufgabe für uns auch sehr wichtig ist – sie setzt nämlich die Verträge auf.

Die Schlüsselperson des Teams ist wahrscheinlich der Project Editor, denn er hält das Team zusammen. Wir haben früher schon mit der unermüdlichen und hochkompetenten Rosemary Caperton zusammengearbeitet und waren sehr erfreut, wieder mit ihr arbeiten zu dürfen. Zu unserer Freude war Rozanne Whalen bereit, das Buch als Fachlektorin zu betreuen, uns auf unsere Schnitzer hinzuweisen und unsere Annahmen zu hinterfragen. Rozanne ist zwar stets unglaublich höflich, aber das sollte niemanden über ihren messerscharfen Verstand hinwegtäuschen.

Für die Qualität und Lesbarkeit eines Buchs ist es unerlässlich, die vorgegebenen sprachlichen und gestalterischen Standards einzuhalten. Wir sind dankbar für die nicht unbeträchtlichen Beiträge, die unser Copyeditor Susan McClung, unsere Korrektorin Nicole Schlutt sowie Maureen Johnson, die Indexerstellerin, und nicht zuletzt Ashley Schneider, die als Projektleiterin bei S4Carlisle Publishing Services alles zusammengehalten hat, geleistet haben.

Kaum ein Mensch ist so ungesellig wie ein Autor, der mitten in einem Buchprojekt steckt, und wir können uns beide glücklich schätzen, so verständnisvolle und hilfsbereite Frauen zu haben. Vielen Dank, Oksana und Anne. Auch ihr seid unverzichtbare und hochgeschätzte Mitglieder des Teams.

Orin and Ian

Einführung

Dieses Training richtet sich an IT-Experten, die in Unternehmensumgebungen für Windows 7 als Desktopbetriebssystem zuständig sind. Sie sollten über mindestens ein Jahr Berufserfahrung verfügen und Erfahrungen mit der Installation und Verwaltung von Windows-Clientbetriebssystemen in einer vernetzten Umgebung gesammelt haben.

Man wird von Ihnen erwarten, dass Sie Aktualisierungen auf Windows 7 durchführen können, wobei Sie die Hardware- und Softwarekompatibilität sicherstellen, und dass Sie Neuinstallationen und Bereitstellungen von Windows 7 erledigen können. Außerdem sollten Sie wissen, wie Sie die vor und nach der Installation des Betriebssystems erforderlichen Einstellungen vornehmen, die Sicherheitsfunktionen von Windows konfigurieren, Netzwerkverbindungen einrichten und die Computer für mobile Benutzer konfigurieren. Weiterhin sollten Sie in der Lage sein, Computer zu warten und Leistungs- und Zuverlässigkeitsprobleme zu erkennen und zu beheben. Außerdem wird es Ihre Arbeit erleichtern, wenn Sie die Windows PowerShell-Syntax in den Grundzügen verstehen.

Beim Durcharbeiten dieses Trainings eignen Sie sich folgende Fähigkeiten an:

- Installieren von Windows 7, Aktualisieren und Migrieren auf Windows 7
- Bereitstellen von Windows 7
- Konfigurieren von Hardware und Anwendungen
- Konfigurieren der Netzwerkverbindungen
- Konfigurieren des Ressourcenzugriffs
- Konfigurieren von Computern für mobile Benutzer
- Überwachen und Warten von Windows 7-Computern
- Konfigurieren der Sicherung und Wiederherstellung



Weitere Informationen **Online-Informationsquellen**

Sobald neues oder aktualisiertes Material zur Verfügung steht, das dieses Buch ergänzt, wird es online auf der Microsoft Press-Online-Windows Server- und Client-Website veröffentlicht (in englischer Sprache). Zu den Dingen, die Sie dort möglicherweise finden, gehören unter anderem Aktualisierungen zum Buchinhalt, Artikel, Links zu begleitendem Inhalt, Errata oder Beispielkapitel. Diese Website steht (in englischer Sprache) unter *http://www.microsoft.com/learning/books/online/serverclient* zur Verfügung.

Einrichten der Testumgebung

Zur Durchführung der Übungen dieses Trainings sind mindestens zwei Clientcomputer oder virtuelle Computer erforderlich, auf denen Windows 7 Enterprise oder Ultimate ausgeführt wird. Eine Anleitung zur Konfiguration des ersten dieser Computer finden Sie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«. Die Beschreibung der Konfiguration des zweiten Computers folgt in Kapitel 6, »Netzwerkeinstellungen«. Außerdem muss der erste der beiden Computer mit einem weiteren Festplattenlaufwerk ausgerüstet werden (intern oder extern), das mit dem NTFS-Dateisystem formatiert wird.

Eine Testversion von Windows 7 Enterprise erhalten Sie im TechNet-Evaluierungscenter von Microsoft unter *http://technet.microsoft.com/de-de/evalcenter/default.aspx*.

Die Computer, auf denen Sie die Übungen dieses Trainings durcharbeiten, müssen die folgenden Systemvoraussetzungen erfüllen.

Hardwarevoraussetzungen

Die meisten Übungen dieses Buchs lassen sich auf virtuellen Computern durchführen. Tabelle 1 nennt die Mindestausstattung und die empfohlene Ausstattung für Windows 7.

Tabelle 1 Hardwarevoraussetzungen für Windows 7

Hardwarekomponente	Mindestausstattung	Empfohlen
Prozessor	x86- oder x64-Prozessor mit einer Taktfrequenz von 1 GHz	2 GHz oder schneller
Arbeitsspeicher	1 GByte	2 GByte
Festplattenplatz	40 GByte	60 GByte
Optisches Laufwerk	DVD-Laufwerk	DVD-Laufwerk
Grafikkarte	Unterstützt DirectX 9 Verfügt über WDDM-Treiber (Windows Display Driver Model) Pixel Shader 2.0-Hardware 32 Bits pro Pixel 128 MByte Grafikspeicher	Wie die Mindestausstattung, allerdings mit 256 MByte Grafikspeicher

Falls Sie beide virtuellen Computer auf demselben Hostcomputer betreiben (empfohlen), sollten Sie einen leistungsfähigeren Computer wählen, um flüssiger arbeiten zu können. Ein Computer mit 4 GByte Arbeitsspeicher und 60 GByte freiem Festplattenspeicher kann alle virtuellen Computer aufnehmen, die in den Übungen dieses Buchs verwendet werden.

Softwarevoraussetzungen

Die Softwarevoraussetzungen sind:

- Windows 7 Enterprise oder Ultimate. Eine Testversion erhalten Sie im TechNet-Evaluierungscenter Center von Microsoft unter *http://technet.microsoft.com/en-us/evalcenter/default.aspx*.
- Für die Übungen aus Kapitel 6, »Netzwerkeinstellungen«, brauchen Sie eine weitere Windows 7-Arbeitsstation. Dafür eignet sich auch ein virtueller Computer.
- Für die optionalen Übungen in Kapitel 14, »Datensicherung und Wiederherstellung«, brauchen Sie ein weiteres Festplattenlaufwerk, das mit dem NTFS-Dateisystem formatiert ist. Dabei kann es sich um ein internes oder ein externes Laufwerk handeln. Es sollte mindestens 20 GByte freien Speicherplatz aufweisen.

Alle Computer müssen an dasselbe Netzwerksegment angeschlossen sein. Wir empfehlen, für die Übungen dieses Buchs ein separates Netzwerk zu verwenden, das nicht mit dem Produktivnetzwerk verbunden ist. Um den Zeitaufwand und die Kosten für den Aufbau der Computer möglichst gering zu halten, empfehlen wir die Verwendung von virtuellen Computern. Wenn Sie unter Windows mit virtuellen Computern arbeiten möchten, können Sie Hyper-V, Microsoft Virtual PC 2007 oder geeignete Software von anderen Herstellern verwenden. Virtual PC 2007 können Sie unter *http://www.microsoft.com/windows/virtual-pc/default.aspx* herunterladen.

Verwenden der Begleit-CD

Die in diesem Buch enthaltene Begleit-CD enthält folgende Komponenten:

- **Übungstests** Mit den Übungstests (in englischer Sprache) können Sie Ihre Kenntnisse über das Konfigurieren von Windows 7 vertiefen. Sie können diese Übungstests an Ihre Anforderungen anpassen, indem Sie die gewünschten Bereiche aus den Lernzielkontrollfragen dieses Buchs auswählen. Oder Sie üben für die Prüfung 70-680 mit Tests, die aus einem Pool von 200 praxisnahen Prüfungsfragen zusammengestellt werden. Diese Zahl reicht aus, um etliche unterschiedliche Testprüfungen durchzuführen, damit Sie optimal vorbereitet sind.
- **E-Books** Elektronische Versionen (E-Books) dieses Buchs in deutscher und englischer Sprache sind auf der Begleit-CD enthalten. So können Sie das Buch auch dann lesen, wenn Sie gerade nicht die Möglichkeit haben, die Papierversion mitzunehmen. Das E-Book liegt im Format PDF (Portable Document Format) vor, Sie können es sich mit Adobe Acrobat oder Adobe Reader ansehen.



Hinweis Wenn Sie dieses Buch ohne Begleitmedium erworben haben (z.B. als E-Book), können Sie die für das Durcharbeiten notwendigen Dateien unter dieser Adresse herunterladen: *http://go.microsoft.com/fwlink/?LinkID=181200*.

So installieren Sie die Übungstests

Gehen Sie folgendermaßen vor, um die Übungstests von der Begleit-CD auf Ihre Festplatte zu installieren:

1. Legen Sie die Begleit-CD in das DVD-Laufwerk. Wenn Sie der Lizenzvereinbarung zustimmen, öffnet sich ein Menü.



Hinweis Falls sich das CD-Menü nicht öffnet

Falls das CD-Menü oder die Lizenzvereinbarung nicht angezeigt wird, ist wahrscheinlich die AutoRun-Funktion auf Ihrem Computer deaktiviert. Bitte lesen Sie in diesem Fall die Datei *Readme.txt* auf der Begleit-CD. Dort finden Sie Hinweise zu alternativen Installationsmethoden.

2. Klicken Sie auf das Feld *Practice Tests* und folgen Sie den angezeigten Anweisungen.

So benutzen Sie die Übungstests

Gehen Sie folgendermaßen vor, um die Übungstests zu starten:

1. Klicken Sie auf *Start/Alle Programme/Microsoft Press Training Kit Exam Prep*.

   Daraufhin öffnet sich ein Fenster, in dem alle Microsoft Press-Training Kit-Prüfungsvorbereitungskomponenten aufgelistet sind, die Sie auf Ihrem Computer installiert haben.
2. Klicken Sie mit einem Doppelklick auf die Lernzielkontroll- oder Übungstests, die Sie durcharbeiten möchten.



Hinweis Unterschiede zwischen Lernzielkontroll- und Übungstests

Wählen Sie den Punkt *Lesson Review* zu *(70-680) Windows 7, Configuring* aus, wenn Sie die Fragen aus den „Lernzielkontrolle"-Abschnitten dieses Buchs durcharbeiten möchten. Wählen Sie den Punkt *Practice Test* aus, wenn Sie Fragen aus einem Pool mit 200 Übungsfragen beantworten möchten, die den Fragen der Prüfung 70-680 ähneln.

Optionen für Lernzielkontrollfragen

Wenn Sie die Lernzielkontrollfragen ausgewählt haben, öffnet sich das Dialogfeld *Custom Mode*, in dem Sie Ihren Test konfigurieren können. Sie können einfach auf *OK* klicken, um die Standardeinstellungen zu übernehmen, oder auswählen, wie viele Fragen gestellt werden sollen, welche Prüfungsziele Sie abdecken wollen und ob die Übungsdauer gemessen werden soll. Falls Sie einen Test ein weiteres Mal durchführen, können Sie auswählen, ob sämtliche Fragen erneut angezeigt werden sollen oder nur die Fragen, die Sie beim letzten Mal falsch oder überhaupt nicht beantwortet haben.

Sobald Sie auf *OK* geklickt haben, beginnt die Lernzielkontrolle.

- Beantworten Sie im Test die Fragen und wechseln Sie mit den Schaltflächen *Next* und *Previous* von einer Frage zur anderen.

- Nachdem Sie eine Frage beantwortet haben, können Sie überprüfen, ob die Antwort richtig war, indem Sie auf die Schaltfläche *Explanation* klicken. Dabei werden auch Erläuterungen zu den richtigen und falschen Antworten angezeigt.
- Falls Sie lieber erst den gesamten Test durcharbeiten wollen, bevor Sie sich das Ergebnis ansehen, können Sie alle Fragen beantworten und dann auf *Score Test* klicken. Daraufhin wird eine Zusammenfassung der ausgewählten Prüfungsziele angezeigt, in der Sie sehen, wie viel Prozent der Fragen Sie insgesamt und pro Lernziel richtig beantwortet haben. Sie können sich den Test ausdrucken, Ihre Antworten durchgehen oder den Test wiederholen.

Optionen für Übungstests

Wenn Sie einen Übungstest starten, können Sie auswählen, ob Sie im Zertifizierungs-, Lern- oder benutzerdefinierten Modus arbeiten wollen:

- **Zertifizierungsmodus (Certification Mode)** Dieser Modus ähnelt dem Ablegen einer echten Zertifizierungsprüfung. Der Test enthält eine bestimmte Zahl von Fragen, die Zeit ist begrenzt und Sie können die Prüfung nicht unterbrechen.
- **Lernmodus (Study Mode)** Erstellt einen Test ohne Zeitbegrenzung, in dem Sie sich die richtigen Antworten und die zugehörigen Erklärungen ansehen können, nachdem Sie jeweils eine Frage beantwortet haben.
- **Benutzerdefinierter Modus (Custom Mode)** In diesem Modus haben Sie volle Kontrolle über die Testoptionen und können den Test nach Belieben gestalten.

Die Benutzeroberfläche beim Durchführen des Tests ist in allen Modi im Wesentlichen dieselbe, allerdings sind jeweils andere Optionen aktiviert oder deaktiviert. Die wichtigsten Optionen wurden im vorhergehenden Abschnitt »Optionen für Lernzielkontrollfragen« beschrieben.

Wenn Sie nachsehen, ob Ihre Antwort für eine einzelne Frage eines Übungstests richtig war, wird ein Verweisabschnitt (*References*) angezeigt, in dem aufgelistet ist, an welcher Stelle im Training das entsprechende Thema behandelt wird und wo Sie weitere Informationen finden. Nachdem Sie auf *Test Results* geklickt haben, um sich das Gesamtergebnis für Ihren Test anzusehen, können Sie auf die Registerkarte *Learning Plan* klicken, um sich eine Liste der Verweise für jedes einzelne Lernziel anzeigen zu lassen.

So deinstallieren Sie die Übungstests

Sie können die Übungstests über das Systemsteuerungsmodul *Programme und Funktionen* deinstallieren.

Das Microsoft Certified Professional-Programm

Die Microsoft-Zertifizierungen bieten Ihnen eine optimale Möglichkeit, Ihre Kenntnisse der aktuellen Microsoft-Produkte und -Technologien unter Beweis zu stellen. Die Prüfungen und entsprechenden Zertifikate dienen als Nachweis Ihrer Kompetenz in Bezug auf Entwurf, Entwicklung, Implementierung und Unterstützung von Lösungen mit Microsoft-Produkten und -Technologien. Fachkräfte, die über Microsoft-Zertifikate verfügen, sind als Experten anerkannt und in der Branche äußerst gefragt. Die Zertifizierung bringt zahlreiche Vorteile für Bewerber, Arbeitgeber und Organisationen mit sich.



Weitere Informationen **Alle Microsoft-Zertifizierungen**

Eine vollständige Liste der Microsoft-Zertifizierungen finden Sie unter *www.microsoft.com/learning/mcp/default.asp*.

Support

Microsoft Press hat sich um die Richtigkeit der in diesem Buch sowie der auf der Begleit-CD enthaltenen Informationen bemüht. Mit Anmerkungen, Fragen oder Verbesserungsvorschlägen zu diesem Buch oder der Begleit-CD können Sie sich an Microsoft Press wenden:

Per E-Mail (auf Englisch):

tkinput@microsoft.com

Per Post:

Microsoft Press
Betrifft: Training 70-680 – Konfigurieren von Windows 7
Konrad-Zuse-Straße 1
85716 Unterschleißheim

Weitere Supportinformationen zu diesem Buch und der beiliegenden CD-ROM finden Sie auf der Supportwebsite von Microsoft Press unter *http://microsoft-press.de/support.asp*. Sie können eine Frage auch direkt in die Microsoft Press Knowledge Base eingeben. Besuchen Sie hierzu die Webseite *http://www.microsoft.com/mspress/support/search.asp*. Weitere Informationen zu den Microsoft-Softwareprodukten erhalten Sie unter der Adresse *http://support.microsoft.com/*.

K A P I T E L 1

Installieren, Migrieren oder Aktualisieren auf Windows 7

Die Prüfung 70-680, »Konfigurieren von Windows 7«, eignet sich für IT-Experten mit mindestens einem Jahr Berufserfahrung in einer vernetzten Umgebung, die im Rahmen ihrer Arbeit das Clientbetriebssystem Windows 7 installieren und unterstützen. Der Schwerpunkt dieses ersten Kapitels liegt auf der Installation von Windows 7, sei es als Neuinstallation oder im Rahmen einer Aktualisierung oder Migration. Als erfahrener IT-Experte wissen Sie, wie wichtig die Installation des Betriebssystems ist. Die Entscheidungen, die Sie im Verlauf der Installation treffen, haben beträchtliche Auswirkungen für die Menschen, die den Computer verwenden.

Dieses Kapitel beschreibt die Installation von Windows 7. Sie lernen die Unterschiede zwischen den verschiedenen Windows 7-Editionen kennen und erfahren, welche Hardwarevoraussetzungen das Betriebssystem stellt, welche Installationsquellen für die Bereitstellung des Betriebssystems verwendet werden können, wie eine Aktualisierung von Windows Vista auf Windows 7 durchgeführt wird und wie Benutzerdaten von Windows XP, Windows Vista und anderen Windows 7-Bereitstellungen übernommen werden können.

In diesem Kapitel abgedeckte Prüfungsziele:

- Durchführen einer Neuinstallation
- Aktualisieren von älteren Windows-Versionen auf Windows 7
- Migrieren der Benutzerprofile

Lektionen in diesem Kapitel:

- Lektion 1: Installieren von Windows 7 3
- Lektion 2: Aktualisieren auf Windows 7 25
- Lektion 3: Verwalten von Benutzerprofilen 34

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels brauchen Sie:

- Zugang zu Hardware, die die in der Einführung dieses Buchs genannten Mindestvoraussetzungen für Windows 7 erfüllt.
- Das Installationsmedium für Windows 7 Enterprise oder Ultimate oder eine Testversion von Windows 7 Enterprise oder Ultimate, die auf der Website von Microsoft erhältlich ist.
- Zur Durchführung der Übung von Lektion 2 brauchen Sie Zugang zu einem Computer, auf dem Windows Vista ausgeführt wird und den Sie auf Windows 7 aktualisieren können. Für diese Übung können Sie einen virtuellen Computer verwenden.
- Für die Übung von Lektion 3 brauchen Sie ein USB-Wechsellaufwerk, das etwa 1 GByte Daten speichern kann.

Praxistipp

Orin Thomas

Leute suchen Rat bei Ihnen als IT-Experte, weil Sie über das Wissen verfügen, das diesen Leuten fehlt. Wenn ein neues Betriebssystem erscheint, werden die Personen, die Ihnen vertrauen, von Ihnen wissen wollen, ob sie dieses Betriebssystem verwenden sollen. Sie möchten wissen, in welchen Punkten es sich von den Betriebssystemen unterscheidet, die sie derzeit verwenden. Sie möchten wissen, ob ihre aktuelle Hardware und Software kompatibel ist oder ob sie einen neuen Computer brauchen. Dieses Buch hat seinen Schwerpunkt zwar im Unternehmensbereich, aber Sie werden aus dem privaten Bereich viele Fragen erhalten, aus der Familie, von Freunden und Kollegen. Wenn Sie gute Ratschläge erteilen möchten, müssen Sie wissen, auf welcher Hardware Windows 7 gut läuft und für welche es sich weniger eignet. Sie müssen entscheiden können, ob sich die Ihnen genannte Hardware und Software für Windows 7 eignet oder ob sie inkompatibel ist. Ob der 5 Jahre alte Multifunktionsdrucker und -scanner auch unter Windows 7 läuft, möchten diese Leute vorher wissen, nicht hinterher, wenn es zu spät ist. Wenn Sie Leuten, die Ihnen vertrauen, einen guten Rat in wichtigen Angelegenheiten geben möchten, ist »gut geraten« nicht gut genug.

Lektion 1: Installieren von Windows 7

Wenn Sie ein Betriebssystem von Anfang an korrekt installieren, ist der spätere Support für das Betriebssystems wesentlich einfacher. Treffen Sie dagegen bei der Installation des Betriebssystems eine falsche Entscheidung und bemerken dies erst nach der Bereitstellung auf Hunderten oder mehr Computern Ihrer Organisation, wird die Bereinigung dieses Problems einige Zeit in Anspruch nehmen. In dieser Lektion erfahren Sie etwas über die Hardwarevoraussetzungen für Windows 7, über die verschiedenen Editionen, über die Durchführung einer Neuinstallation und darüber, wie man Windows 7 neben weiteren Betriebssystemen auf demselben Computer installiert.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Windows 7-Hardwarevoraussetzungen benennen
- Konfigurieren von Windows 7 als einziges Betriebssystem eines Computers
- Konfigurieren von Windows 7 für Dual-Boot
- Starten vom Installationsmedium
- Vorbereitungen für die Installation von USB, CD, Netzwerkfreigabe oder mit den Windows-Bereitstellungsdiensten

Veranschlagte Zeit für diese Lektion: 70 Minuten

Windows 7-Editionen

Es gibt mehrere Editionen des Betriebssystems Windows 7. Gelegentlich werden Sie für diese unterschiedlichen Editionen auch die Bezeichnung SKUs (Stock Keeping Units) sehen. Microsoft legt diese verschiedenen Editionen für verschiedene Verwendungszwecke aus. Kunden, die nicht alle Funktionen brauchen, die in einer teureren Edition verfügbar sind, erhalten auf diese Weise zum Beispiel eine preisgünstigere Version von Windows 7. Es gehört vermutlich zu Ihren Aufgaben als IT-Experte, Ihre Organisation bei der Auswahl der anzuschaffenden Edition von Windows 7 zu beraten. Wahrscheinlich werden Sie auch Ihre Familie und Ihre Freunde bei der Wahl der passenden Windows 7-Edition beraten müssen. Es gibt sechs verschiedene Editionen von Windows 7:

- Starter
- Home Basic
- Home Premium
- Professional
- Enterprise
- Ultimate

Auf den nächsten Seiten werden die wichtigsten Unterschiede zwischen diesen Editionen beschrieben.

Windows 7 Starter

Windows 7 Starter ist im Einzelhandel und in Kombination mit neuen Computern erhältlich, auf denen es bereits von den Computerherstellern installiert wird. Es enthält oder unterstützt folgende Funktionen nicht: die Benutzerschnittstelle Windows Aero, die Wiedergabe von

DVDs, das Windows Media Center und die gemeinsame Verwendung von Internetverbindungen. Einen Computer mit dieser Edition von Windows können Sie auch nicht in eine Domäne aufnehmen. Diese Edition unterstützt keine Unternehmensfunktionen wie das verschlüsselnde Dateisystem (Encrypting File System, EFS), AppLocker, DirectAccess, BitLocker, den Remotedesktophost oder BranchCache. Diese Edition unterstützt maximal einen physischen Prozessor.

Windows 7 Home Basic

Windows 7 Home Basic ist nur in Schwellenländern erhältlich. Es enthält oder unterstützt folgende Funktionen nicht: die Benutzerschnittstelle Windows Aero, die Wiedergabe von DVDs, das Windows Media Center oder den IIS-Webserver. Einen Computer mit dieser Edition von Windows 7 können Sie auch nicht in eine Domäne aufnehmen. Diese Edition unterstützt keine Unternehmensfunktionen wie EFS, AppLocker, DirectAccess, BitLocker, den Remotedesktophost oder BranchCache. Sie unterstützt maximal einen physischen Prozessor. Die x86-Version unterstützt maximal 4 GByte Arbeitsspeicher, während die x64-Version maximal 8 GByte Arbeitsspeicher unterstützt.



Hinweis **Multiprozessor und Multikern**

Einige Editionen unterstützen zwar nur einen physischen Prozessor, aber sie unterstützen trotzdem eine unbegrenzte Zahl von Prozessorkernen. So unterstützen zum Beispiel alle Windows 7-Editionen Quad-Core-CPUs.

Windows 7 Home Premium

Windows 7 Home Premium ist im Einzelhandel und vorinstalliert auf neuen Computern erhältlich. Im Gegensatz zu den Editionen Starter und Home Basic unterstützt die Home Premium-Edition die Benutzeroberfläche Windows Aero, die DVD-Wiedergabe, das Windows Media Center, die gemeinsame Verwendung von Internetverbindungen und den IIS-Webserver. Aber auch diese Edition von Windows 7 können Sie nicht in eine Domäne aufnehmen und sie unterstützt keine Unternehmensfunktionen wie EFS, AppLocker, DirectAccess, BitLocker, den Remotedesktophost und BranchCache. Die x86-Version von Windows 7 Home Premium unterstützt maximal 4 GByte Arbeitsspeicher, die x64-Version maximal 16 GByte. Windows 7 Home Premium unterstützt bis zu zwei physische Prozessoren.

Windows 7 Professional

Windows 7 Professional ist im Einzelhandel und vorinstalliert auf neuen Computern erhältlich. Die Edition bietet alle Funktionen, die auch in Windows Home Premium verfügbar sind. Darüber hinaus können Computer, auf denen Windows 7 Professional ausgeführt wird, in eine Domäne aufgenommen werden. Es unterstützt EFS und den Remotedesktophost, aber keine Unternehmensfunktionen wie AppLocker, DirectAccess, BitLocker und BranchCache. Windows 7 Professional unterstützt bis zu zwei physische Prozessoren.

Windows 7 Enterprise und Ultimate

Die Editionen Windows 7 Enterprise und Ultimate sind bis auf die Tatsache identisch, dass Windows 7 Enterprise nur für Volumenlizenzkunden von Microsoft erhältlich ist, während es Windows 7 Ultimate im Einzelhandel und vorinstalliert auf neuen Computern gibt. Die Editionen Enterprise und Ultimate bieten alle Funktionen, die auch in anderen Windows 7-Editionen verfügbar sind, und unterstützen darüber hinaus alle Unternehmensfunktionen wie

EFS, den Remotedesktophost, AppLocker, DirectAccess, BitLocker, BranchCache und das Starten von VHD. Die Editionen Windows 7 Enterprise und Ultimate unterstützen bis zu zwei physische Prozessoren.



Prüfungstipp

Viele der Windows 7-Funktionen, nach denen in der Prüfung 70-680 gefragt wird, sind nur in den Editionen Enterprise und Ultimate von Windows 7 verfügbar.

Hardwarevoraussetzungen für Windows 7

Betriebssysteme funktionieren nur dann mit akzeptabler Leistung, wenn die Computer, auf denen sie installiert werden, die Mindestanforderungen erfüllen, die das Betriebssystem an die Hardware stellt. Diese Voraussetzungen gelten aber nur für das Betriebssystem selbst. Gewöhnlich wollen Benutzer aber mehr tun, als nur das Betriebssystem zu verwenden, sie wollen auch noch mit Anwendungen arbeiten. Anwendungen erfordern Arbeitsspeicher und Speicherplatz auf der Festplatte, der über die Mindestanforderungen des Betriebssystems hinausgeht. Wenn Sie in Ihrer Organisation Empfehlungen zur Spezifikation der Computerhardware abgeben müssen, die Ihre Organisation beschaffen soll, müssen Sie nicht nur die Anforderungen des Betriebssystems berücksichtigen, sondern auch die zusätzlichen Anforderungen der Anwendungen, die auf den Computern ausgeführt werden sollen. Für Windows 7 Starter und Windows 7 Home Basic gelten folgende Hardwarevoraussetzungen:

- 1-GHz-Prozessor, 32 Bit (x86) oder 64 Bit (x64)
- 512 MByte Arbeitsspeicher
- Ein herkömmliches Festplattenlaufwerk mit mindestens 20 GByte (x64) oder 16 GByte (x86) Speicherplatz, oder eine SSD (Solid State Disk) mit mindestens 15 GByte freiem Speicherplatz
- Eine Grafikkarte mit 32 MByte Grafikspeicher, die DirectX 9 unterstützt

Windows 7 Home Premium, Professional, Ultimate und Enterprise stellen folgende Anforderungen an die Hardware:

- 1-GHz-Prozessor, 32 Bit (x86) oder 64 Bit (x64)
- 1 GByte Arbeitsspeicher
- Ein herkömmliches Festplattenlaufwerk mit mindestens 40 GByte Speicherplatz oder eine SSD mit mindestens 15 GByte freiem Speicherplatz
- Eine Grafikkarte, die DirectX 9 unterstützt, über WDDM-Treiber (Windows Display Driver Model), Pixel Shader 2.0-Hardware und 128 MByte Grafikspeicher verfügt und 32 Bits pro Pixel verwenden kann

Windows 7 unterstützt zwei verschiedene Prozessorarchitekturen. Die 32-Bit-Version von Windows 7 wird gewöhnlich x86 genannt. Die x86-Version von Windows 7 sollten Sie auf Computern installieren, die ältere Prozessoren wie zum Beispiel den Pentium IV haben, sowie auf neuen Laptops mit kleinem Formfaktor, die auch *Netbooks* genannt werden. Die wichtigste Beschränkung der x86-Version von Windows 7 liegt darin, dass sie nicht mehr als 4 GByte Arbeitsspeicher unterstützt. Die x86-Version von Windows 7 lässt sich zwar auch auf Computern mit x64-Prozessoren installieren, aber das Betriebssystem ist dann trotzdem nicht in der Lage, mehr als 4 GByte Arbeitsspeicher zu verwenden. Die x64-Version von

Windows 7 können Sie nur auf Computern installieren, die über einen x64-kompatiblen Prozessor verfügen. Die x64-Versionen von Windows 7 Professional, Enterprise und Ultimate unterstützen bis zu 128 GByte Arbeitsspeicher. Die x64-Version von Windows 7 Home Basic unterstützt 8 GByte und die x64-Version von Home Premium maximal 16 GByte.

Schnelltest

- Was ist der Unterschied zwischen den Editionen Windows 7 Enterprise und Ultimate?

Antwort zum Schnelltest

- Der Unterschied liegt in den Lizenzbedingungen. Windows 7 Enterprise kann nur von Organisationen verwendet werden, die entsprechende Unternehmenslizenzverträge mit Microsoft abschließen. Windows 7 Ultimate gibt es als herkömmliche Einzelhandelslizenz.

Vorbereiten der Windows 7-Installationsquelle

Sie können bei der Installation von Windows 7 unter mehreren Methoden wählen. Welche die beste ist, hängt von der Situation ab. Die Installation von DVD ist sinnvoll, wenn es nur um einige Computer geht. Müssen Sie Windows 7 auf 20 oder mehr Computern bereitstellen, sollten Sie eine Methode wählen, die sich für die Bereitstellung auf vielen Computern eignet. Berücksichtigen Sie bei der Wahl der Installationsquelle folgende Faktoren:

- Müssen Sie Windows 7 auf mehr als einem Computer bereitstellen?
- Verfügen der oder die Computer über DVD-Laufwerke?
- Müssen Sie eine angepasste Version von Windows 7 bereitstellen?
- Möchten Sie den Installationsvorgang automatisieren?

Verwenden einer DVD als Installationsquelle

Wenn Sie Windows 7 im Einzelhandel kaufen, erhalten Sie es mit einer DVD als Datenträger. Manche Unternehmenskunden haben auch Zugang zu einem speziellen Bereich der Microsoft-Website, in dem Sie ein DVD-Abbild von Windows 7 im ISO-Format (International Organization for Standardization) herunterladen können. Dieses Abbild müssen Sie auf eine DVD brennen, um Windows 7 installieren zu können.

Zur Installation von Windows 7 von DVD starten Sie den Computer von der DVD und folgen den Dialogfeldern des Installationsassistenten. Wahrscheinlich müssen Sie vorher das BIOS des Computers so einstellen, dass ein Start des Computers von DVD möglich ist. Verfügt der Computer über kein eingebautes DVD-Laufwerk, können Sie trotzdem eine Installation von DVD durchführen, wenn Sie ein USB-DVD-Laufwerk anschließen. In diesem Fall ist es erforderlich, das BIOS des Computers so einzustellen, dass der Start vom USB-Laufwerk erfolgt.

Eine Installation von DVD ist die einfachste Lösung, wenn Windows 7 nur auf wenigen Computern installiert werden soll und das Betriebssystemabbild vorher nicht angepasst werden muss.

Verwenden eines USB-Laufwerks als Installationsquelle

Computer mit kleinem Formfaktor, meistens *Netbookcomputer* oder *Netbooks* genannt, werden immer beliebter. Für den IT-Experten haben diese Computer aber den Nachteil, dass

sie wegen ihrer geringen Größe häufig nicht über ein optisches Laufwerk verfügen. Es ist zwar meist möglich, ein externes USB-DVD-Laufwerk anzuschließen und die Installation durchzuführen, aber die Administratoren steigen zunehmend um auf billige USB-Speichergeräte, auch *Flashlaufwerke* genannt, die mit mehreren GByte Speicherkapazität erhältlich sind.

USB-Speichergeräte haben gegenüber DVDs mehrere Vorteile. Mit Tools wie *Dism.exe* können Sie das Betriebssystemabbild auf einem USB-Speichergerät direkt ändern. Sie können zusätzliche Treiber zu dem auf dem USB-Speichergerät gespeicherten Abbild hinzufügen, was bei einem Abbild, das auf DVD gespeichert ist, nicht möglich ist. Wie das geschieht, erfahren Sie in Kapitel 3, »Bereitstellen von Systemabbildern«. Ein weiterer Vorteil der USB-Flashlaufwerke ist ihre höhere Lesegeschwindigkeit. Die Übertragung der Betriebssystemdateien auf den Zielcomputer erfolgt schneller als bei der Installation von DVD.

Wenn Sie ein USB-Speichergerät als Installationsquelle für Windows 7 verwenden möchten, muss es mindestens 4 GByte Daten aufnehmen können, denn die x64-Installationsdateien sind etwa 3,2 GByte groß, die x86-Installationsdateien ungefähr 2,5 GByte. Bei der Vorbereitung der Installation vom USB-Speichergerät verwenden Sie nur die Installationsdateien einer Architektur. Das USB-Speichergerät sollte mit dem Dateisystem FAT32 formatiert werden.

So bereiten Sie ein USB-Speichergerät als Installationsquelle für Windows 7 vor:

1. Verbinden Sie das USB-Speichergerät mit einem Computer, auf dem Windows Vista oder Windows 7 ausgeführt wird. Wenn das Speichergerät Daten enthält, die Sie behalten möchten, sichern Sie die Daten auf einem anderen Gerät, denn bei der Vorbereitung des Geräts als Installationsquelle gehen alle enthaltenen Daten verloren.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben Sie **diskpart** ein**.**
3. Geben Sie an der *DISKPART*>-Eingabeaufforderung **list disk** ein**.** Überprüfen Sie, bei welcher Festplatte es sich um das USB-Speichergerät handelt.
4. Geben Sie an der *DISKPART*>-Eingabeaufforderung **select disk X** ein, wobei *X* die Nummer der Festplatte ist, die Sie als USB-Speichergerät identifiziert haben.
5. Geben Sie an der *DISKPART*>-Eingabeaufforderung **clean** ein. Wenn die Festplatte gelöscht ist, geben Sie **create partition primary** ein**.**
6. Geben Sie an der *DISKPART*>-Eingabeaufforderung **format fs=fat32 quick** ein**.** Nach dem Abschluss der Formatierung geben Sie **active** ein und dann **exit.**
7. Kopieren Sie nun alle Dateien von der Installations-DVD von Windows 7 auf das USB-Speichergerät.
8. Konfigurieren Sie im BIOS des Computers, auf dem Sie Windows 7 installieren möchten, den Start vom USB-Speichergerät. Schließen Sie das USB-Speichergerät an und starten Sie den Computer neu, um die Installation durchzuführen.

Allerdings bringt die Verwendung von USB-Speichergeräten als Windows 7-Installationsquelle auch einige Nachteile mit sich. USB-Speichergeräte sind zwar wiederverwendbar, aber auch teurer als DVD-ROMs. USB-Speichergeräte sind wie DVDs nicht die erste Wahl, wenn Windows 7 in kurzer Zeit auf einer großen Zahl von Computern installiert werden soll, weil Sie für die Installation an jedem Computer ein USB-Speichergerät anschließen müssen. Wenn Sie zum Beispiel Windows 7 auf 100 Computern bereitstellen möchten, könnten Sie

100 USB-Speichergeräte mit den Installationsdateien von Windows 7 und den Antwortdateien für eine unbeaufsichtigte Installation vorbereiten, oder Sie könnten einen Windows-Bereitstellungsdiensteserver aufbauen und die Installation über das Netzwerk hinweg durchführen – eine wesentlich praktischere Alternative.

Verwenden einer Netzwerkfreigabe als Installationsquelle

Als Alternative zu DVDs oder USB-Speichergeräten können Sie die Windows 7-Installationsdateien in einer Netzwerkfreigabe speichern. Kopieren Sie den Inhalt des Windows 7-Installationsmediums auf eine Netzwerkfreigabe, die für die Clients zugänglich ist, auf denen Sie Windows 7 installieren möchten. Um die Netzwerkfreigabe auf dem Clientcomputer als Installationsquelle verwenden zu können, müssen Sie den Clientcomputer mit der Windows-Vorinstallationsumgebung starten. Die Windows-Vorinstallationsumgebung (Windows Preinstallation Environment, Windows PE) ist ein kleines Betriebssystem, das den Einsatz von Diagnose- und Wartungstools sowie den Zugriff auf Netzwerkfreigaben ermöglicht. Nach dem erfolgreichen Start von Windows PE können Sie eine Verbindung mit der Netzwerkfreigabe herstellen und die Installation mit *Setup.exe* starten. Wie eine startfähige Windows PE-DVD oder ein entsprechendes USB-Speichergerät erstellt wird, erfahren Sie in Kapitel 2, »Konfigurieren von Systemabbildern«.

Da der Start von Windows PE erforderlich ist, hat eine Netzwerkfreigabe als Installationsquelle gegenüber einer Installation mit DVDs oder USB-Speichergeräten einige Nachteile. Obwohl die Installationsdateien des Betriebssystems in einer Netzwerkfreigabe liegen, brauchen Sie trotzdem noch eine DVD oder müssen ein USB-Speichergerät an den Computer anschließen. Netzwerkinstallationen dieser Art sind außerdem langsamer als vergleichbare Installationen von DVD oder von einem USB-Speichergerät, weil die Installationsdateien über das Netzwerk übertragen werden müssen.

Allerdings hat eine Netzwerkfreigabe als Installationsquelle auch den Vorteil, dass Änderungen zentral erfolgen können. Wenn Sie an einer USB-Quelle eine Änderung durchführen möchten, müssen Sie jede einzelne USB-Quelle aktualisieren. Wenn Sie an einer DVD-Quelle eine Änderung durchführen möchten, müssen Sie alle DVDs neu brennen. Es ist nicht erforderlich, auch das Windows PE-Medium zu ändern, das Sie für den Start der Clientcomputer verwenden, wenn Sie die zentrale Quelle aktualisieren. Außerdem können Sie eine Netzwerkfreigabe auch dann als Installationsquelle verwenden, wenn Ihre Organisation nicht über eine Active Directory-Domänendienste-Infrastruktur verfügt oder keine Server hat, auf denen das Betriebssystem Windows Server 2008 verwendet wird.

Verwenden der Windows-Bereitstellungsdienste als Installationsquelle

Wenn Sie eine größere Zahl von Installationen über das Netzwerk durchführen möchten und Ihnen die Active Directory-Domänendienste und Windows Server 2008 zur Verfügung stehen, kommen die Windows-Bereitstellungsdienste in Betracht. Sie sind unter Windows Server 2008 als Rolle verfügbar und ermöglichen die automatische Bereitstellung von Betriebssystemabbildern. Die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS) können Multicast-Übertragungen verwenden. Das bedeutet, dass das Abbild nicht einzeln zu jedem Computer übertragen wird, auf dem Windows 7 installiert werden soll. Unter optimalen Bedingungen übermitteln die WDS das Betriebssystem stattdessen mit einer einzigen Übertragung an alle Computer, die es erhalten sollen.

Für den Zugriff auf den Windows-Bereitstellungsdiensteserver braucht ein Clientcomputer eine PXE-konforme Netzwerkkarte oder muss von einem WDS-Suchabbild gestartet wer-

den. Wenn der Computer von einer PXE-konformen Netzwerkkarte oder von einem Suchabbild gestartet wird, stellt er eine Verbindung mit dem Windows-Bereitstellungsdiensteserver her und kann mit der Bereitstellung des Betriebssystems beginnen. Bei der Vorbereitung des Windows-Bereitstellungsdiensteservers wird das Installationsabbild *Install.wim* vom Windows 7-Installationsmedium auf den Server kopiert. Sie kopieren die Installationsdateien nicht über das Netzwerk, wie Sie es bei der Vorbereitung einer Netzwerkfreigabe oder eines USB-Speichergeräts tun würden.

Sie können auf dem Windows-Bereitstellungsdiensteserver auch eine Datei für die unbeaufsichtigte Installation vorbereiten und die Betriebssystemabbilder auf dem Windows-Bereitstellungsdiensteserver ändern. Über die Bereitstellung von angepassten Windows 7-Abbildern erfahren Sie mehr in Lektion 2 von Kapitel 3.



Weitere Informationen Windows-Bereitstellungsdienste

Weitere Informationen über die WDS finden Sie im Microsoft TechNet auf folgender Webseite: *http://technet.microsoft.com/en-us/library/cc265612.aspx.*



Prüfungstipp

Merken Sie sich, welche Art von Installationsquelle Sie in welcher Situation verwenden.

Installieren von Windows 7

Die Installation von Windows 7 ist nicht schwer. Sie starten den Installationsvorgang, indem Sie den Computer von einer DVD oder einem USB-Speichergerät starten, eine Verbindung mit dem Windows-Bereitstellungsdiensteserver herstellen oder den Computer in Windows PE starten, eine Verbindung mit einer Netzwerkfreigabe herstellen und *Setup.exe* starten. Anschließend können Sie eine Standardinstallation oder eine unbeaufsichtigte Installation durchführen:

- **Standardinstallation** Im Verlauf einer Standardinstallation beantwortet ein Administrator eine Reihe von Fragen und legt dadurch fest, wie Windows 7 auf dem neuen Computer installiert werden soll. Diese Installationsart ist sehr gut geeignet, um Windows 7 auf einer kleinen Anzahl von Computern bereitzustellen.
- **Unbeaufsichtigte Installation** Mit einer Installationsdatei namens *Unattend.xml* können Sie Windows 7 ohne Aufsicht installieren. In dieser Installationsdatei sind die Antworten auf die Fragen gespeichert, die der Installationsassistent stellt. Beim Start der Installation überprüft der Installationsassistent, ob es angeschlossene USB-Speichergeräte gibt, in deren Stammverzeichnis diese Datei liegt. Unbeaufsichtigte Installationen sind vor allem dann sinnvoll, wenn Sie Windows 7 auf einer großen Zahl von Computern installieren müssen, weil Sie dann nicht auf jedem einzelnen Computer die Fragen beantworten müssen, die im Verlauf der Installation gewöhnlich gestellt werden.

Neuinstallationen

Eine Neuinstallation ist eine Installation, die auf einem Computer durchgeführt wird, auf dem noch kein Betriebssystem installiert ist. Dabei kann es sich zum Beispiel um einen brandneuen Computer direkt vom Hersteller handeln, oder um einen älteren Computer mit einem neuen Festplattenlaufwerk, auf dem Sie Windows 7 installieren möchten. Eine Neu-

installation können Sie mit jedem Installationsmedium durchführen. In der Übung am Ende dieses Kapitels wird zwar eine Neuinstallation durchgeführt, aber die nächsten Seiten beschreiben etwas ausführlicher einige der Optionen und Konzepte, denen Sie bei der Installation begegnen.

Auf der ersten Seite des Installationsassistenten werden Sie gefragt, welche Sprache installiert werden soll, in welchem Format Datum und Uhrzeit angezeigt werden sollen und welche Tastatur oder Eingabemethode Sie für die Installation verwenden möchten. Diese Auswahl ist nicht nur deswegen wichtig, weil die Installation von Microsoft Windows in einer Fremdsprache durchaus zur Herausforderung werden kann, wenn Sie diese Fremdsprache nicht verstehen, aber auch weil selbst in Ländern, in denen dieselbe Sprache gesprochen wird, zum Teil unterschiedliche Tastaturen verwendet werden. Wenn Sie Windows 7 für Benutzer installieren, die mit unterschiedlichen Tastaturen arbeiten, können Sie die fehlenden Tastaturlayouts nach dem Abschluss der Installation hinzufügen. Anschließend können die Benutzer nach Bedarf zwischen den verfügbaren Tastaturlayouts wechseln.

Die nächste Seite ist die Installationsseite für Windows 7 (Abbildung 1.1). Von hier aus können Sie die Installation mit einem Klick auf *Jetzt installieren* einleiten. Wenn Sie auf *Computerreparaturoptionen* klicken, erhalten Sie Zugriff auf die Reparaturtools von Windows 7. Über die Reparaturoptionen erfahren Sie mehr in Kapitel 14, »Datensicherung und Wiederherstellung«. Ein Klick auf die Option *Wissenswertes vor der Windows-Installation* liefert allgemeine Hinweise für die Installation. Sie erfahren zum Beispiel, dass der Computer die Systemvoraussetzungen erfüllen muss und dass Sie den Product Key bereitlegen sollten.

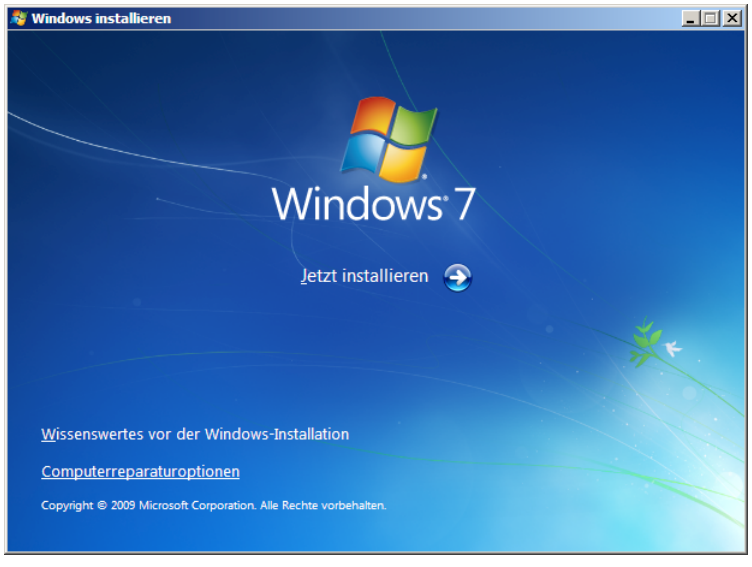


Abbildung 1.1 Die Installationsseite für Windows 7

Der nächste Schritt ist die Prüfung der Lizenzbedingungen für Windows 7. Wenn Sie die Lizenzbedingungen akzeptieren, werden Sie auf der folgenden Seite gefragt, welche Art von Installation Sie durchführen möchten, *Upgrade* oder *Benutzerdefiniert (erweitert)*. Zur Durchführung einer Neuinstallation sollten Sie *Benutzerdefiniert (erweitert)* wählen. Die

meisten Installationen von Windows 7, die Sie durchführen werden, sind wahrscheinlich vom Typ *Benutzerdefiniert (erweitert)* und keine Upgrades. Upgrade-Installationen können Sie nur unter Windows Vista oder Windows 7 durchführen. Über die Aktualisierung von Windows 7 erfahren Sie mehr in Lektion 2.

Im nächsten Schritt der Installation legen Sie fest, wo die Windows 7-Dateien gespeichert werden. Windows 7 braucht mindestens 15 GByte freien Speicherplatz. Allerdings sollten Sie mehr als nur diese Menge vorsehen. Auf dieser Seite ist es möglich, eine vorhandene Festplatte in kleinere Volumes aufzuteilen. Dazu klicken Sie auf *Laufwerksoptionen (erweitert)*. Die Installationsroutine erkennt automatisch die meisten Festplattenlaufwerke der Typen IDE (Integrated Drive Electronics), SATA (Serial Advanced Technology Attachment) und SCSI (Small Computer System Interface). Wenn Ihr Computer mit spezieller Festplattenhardware ausgestattet ist, beispielsweise mit einem RAID-System (Redundant Array of Independent Disks), müssen Sie vielleicht die Option *Treiber laden* verwenden. Allerdings brauchen Sie diese Option nur zu verwenden, wenn die Festplatte, auf der Sie Windows installieren möchten, nicht als für die Installation benutzbarer Datenträger angezeigt wird. Wird Ihre Festplatte dagegen als verfügbare Option angezeigt, hat Windows 7 bereits die passenden Treiber geladen. Nachdem Sie den Ort festgelegt haben, an dem Windows 7 installiert werden soll, beginnt die Installation.



Hinweis Installieren auf VHD

Bei einer Neuinstallation von Windows 7 Enterprise oder Ultimate haben Sie außerdem die Wahl, das Betriebssystem nicht direkt auf einem Volume der physischen Festplatte zu installieren, sondern auf einer virtuellen Festplatte – anders gesagt, in einer VHD-Datei (Virtual Hard Disk). Welche Schritte dafür erforderlich sind, erfahren Sie in Kapitel 2.

Nach dem Neustart des Computers müssen Sie einen Benutzer- und einen Computernamen festlegen. Der Benutzername, den Sie festlegen, wird als Name des Standardadministratorkontos für den Computer verwendet. Das Konto mit dem Namen *Administrator*, das in älteren Windows-Versionen als Standardadministratorkonto verwendet wurde, wird standardmäßig deaktiviert. Es lässt sich nur durch eine Änderung der Gruppenrichtlinien wieder aktivieren. Da der Benutzername, den Sie bei der Installation angeben, für das Standardadministratorkonto des Computers verwendet wird, müssen Organisationen, die eine Windows 7-Bereitstellung durchführen, auch Regeln für die Namensgebung festlegen. Die meisten Organisationen lassen aus Sicherheitsgründen nicht zu, dass die Personen, die an den Computern arbeiten, über Administratorrechte verfügen. Einheitliche Regeln für die Benennung des Standardadministratorkontos sorgen außerdem dafür, dass die IT-Experten bei der Anmeldung als lokaler Administrator nicht raten müssen, wie das Administratorkonto wohl heißen mag. Bei Bereitstellungen in Organisationen ist es auch erforderlich, einheitliche Regeln für die Benennung der Computer festzulegen. Computer- und Benutzernamen dürfen keine Sonderzeichen enthalten (Abbildung 1.2).

Nachdem Sie einen Benutzer- und einen Computernamen angegeben haben, ist es erforderlich, ein Kennwort und einen Kennworthinweis einzugeben. Da es sich bei diesem Benutzerkonto um das Standardadministratorkonto für den Windows 7-Computer handelt, sollte der Kennworthinweis es auch cleveren Leuten nicht ermöglichen, das Kennwort zu erraten. Kennworthinweise für lokale Benutzerkonten können alle Benutzer einsehen, die sich lokal am Computer anmelden möchten, und das kann ein Sicherheitsrisiko darstellen.

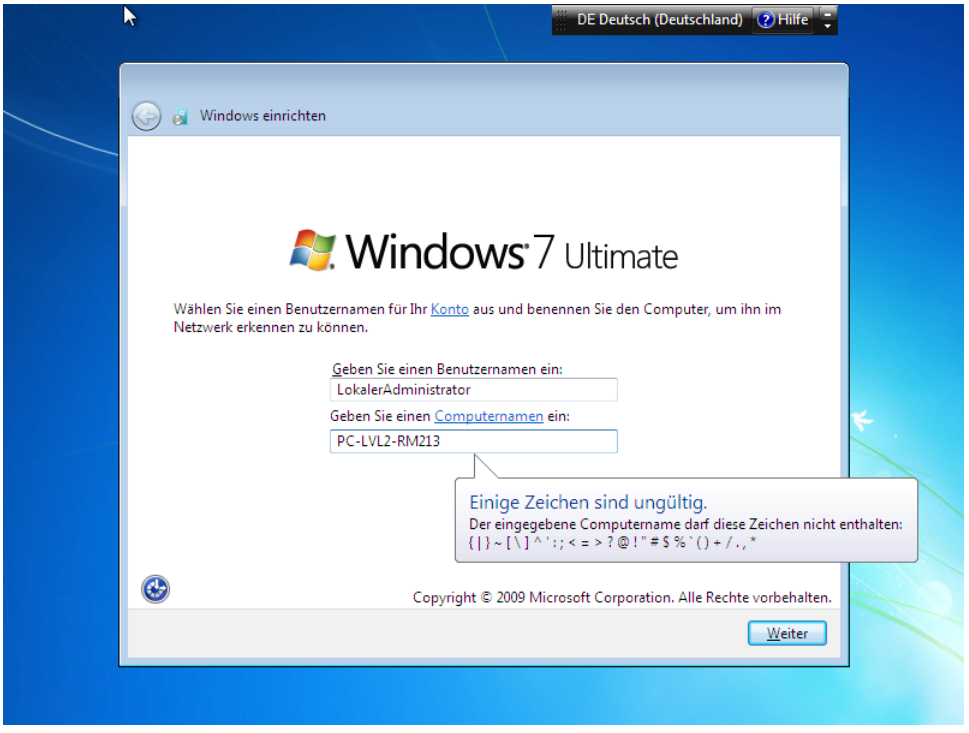

DE Deutsch (Deutschland)
Hilfe
Windows einrichten
Windows 7 Ultimate
Wählen Sie einen Benutzernamen für Ihr Konto aus und benennen Sie den Computer, um ihn im Netzwerk erkennen zu können.
Geben Sie einen Benutzernamen ein:
LokalerAdministrator
Geben Sie einen Computernamen ein:
PC-LVL2-RM213
Einige Zeichen sind ungültig.
Der eingegebene Computername darf diese Zeichen nicht enthalten:
{ | } ~ [\ ] ^ ' : ; < = > ? @ ! " # $ % ` ( ) + / . , *
Copyright © 2009 Microsoft Corporation. Alle Rechte vorbehalten.
Weiter

Abbildung 1.2 Benutzer- und Computernamen dürfen keine Sonderzeichen enthalten

Im nächsten Schritt erhalten Sie die Gelegenheit, den Product Key einzugeben und Windows so zu konfigurieren, dass es sich nach dem Abschluss der Installation bei der nächsten Gelegenheit automatisch aktiviert, sobald eine Verbindung mit dem Internet zustande kommt. Wie Sie wissen, haben Sie 30 Tage Zeit für die Produktaktivierung, Sie brauchen sie also nicht unmittelbar nach der Installation durchzuführen. Nutzen Sie diese 30 Tage, um zu überprüfen, ob die Software- und Hardwarekonfiguration des Computers die Erwartungen erfüllt. Führen Sie die Produktaktivierung erst durch, wenn Sie damit zufrieden sind.

Wenn Sie jetzt einen Product Key eingeben, sollten Sie darauf achten, dass er zu der von Ihnen erworbenen Edition passt. Wenn Sie zum Beispiel nur einen Product Key für Windows 7 Home Premium zur Verfügung haben, aber Windows 7 Ultimate installieren, müssen Sie entweder noch einen Schlüssel für die Ultimate-Edition erwerben oder Windows 7 noch einmal installieren.

Nach diesem Schritt erscheint die Seite *Schützen Sie Ihren Computer, und verbessern Sie Windows automatisch* (Abbildung 1.3). Wenn Sie Installationen in einer Umgebung durchführen, in denen es keine automatische Updatelösung wie WSUS (Windows Software Update Services) gibt, sollten Sie die Option *Empfohlene Einstellungen verwenden* wählen. Allerdings sollten Sie berücksichtigen, dass der Windows 7-Computer dann eine Internetverbindung verwendet, um direkt nach dem Abschluss der Installation die wichtigen und empfohlenen Updates herunterzuladen. Das kann sich stark auf die Bandbreitenverwendung der externen Verbindungen auswirken, wenn Sie Windows 7 auf einer größeren Anzahl von Computern installieren. In solchen Fällen sollten Sie die Bereitstellung von WSUS oder einer vergleichbaren Lösung in Betracht ziehen. Außerdem ist es möglich, Updates zum

Installationsabbild hinzuzufügen, bevor Sie es bereitstellen. Dieser Vorgang wird in Kapitel 3 beschrieben. Wie man Windows 7 nach der Bereitstellung aktualisiert, erfahren Sie in Kapitel 12, »Windows Update und Windows Internet Explorer«.


Windows einrichten
Schützen Sie Ihren Computer, und verbessern Sie Windows automatisch.
Empfohlene Einstellungen verwenden
Wichtige und empfohlene Updates installieren, zur sicheren Verwendung des Internets beitragen, online nach Problemlösungen suchen und Microsoft bei der Optimierung von Windows unterstützen.
Nur wichtige Updates installieren
Nur Sicherheitsupdates bzw. andere wichtige Updates für Windows installieren.
Später erneut nachfragen
Solange Sie sich nicht entscheiden, wird die Computersicherheit eventuell beeinträchtigt.
Weitere Informationen über jede Option
Wenn Sie die empfohlenen Einstellungen verwenden oder nur Updates installieren, werden einige Informationen an Microsoft gesendet. Die Informationen werden jedoch nicht verwendet, um Sie zu identifizieren oder Kontakt mit Ihnen aufzunehmen. Wenn Sie diese Einstellungen zu einem späteren Zeitpunkt deaktivieren möchten, suchen Sie unter "Hilfe und Support" nach "Empfohlene Einstellungen deaktivieren". Lesen Sie die Datenschutzbestimmungen.

Abbildung 1.3 Festlegen der Updateeinstellungen

In der nächsten Installationsphase wird festgelegt, zu welcher Zeitzone der Computer gehört und ob die Sommerzeit automatisch berücksichtigt werden soll. Außerdem zeigt der Computer das Datum und die Uhrzeit an. Diese Einstellungen können Sie bei Bedarf korrigieren. Nach dem Anschluss des Computers an ein Netzwerk übernimmt der Computer Datum und Uhrzeit automatisch von einem Server aus dem lokalen Netzwerk, sofern er Mitglied einer Windows-Domäne ist, oder von einem Zeitserver im Internet, falls er nicht Mitglied einer Domäne ist.

Wenn das Installationsprogramm während der Installation ein Netzwerk erkennt, geben Sie an, ob es sich bei dem Netzwerk um ein *Heimnetzwerk*, ein *Arbeitsplatznetzwerk* oder ein *Öffentliches Netzwerk* handelt (Abbildung 1.4). Von dem Netzwerktyp, den Sie wählen, hängt es ab, welche Dienste auf dem Windows 7-Computer verfügbar sind und auf welche Orte im Netzwerk ein Windows 7-Computer Zugriff erhält, beispielsweise auf die Heimnetzgruppe. Wenn Sie die Einstellung *Heimnetzwerk* wählen, können Sie je nach Installationsquelle die Bibliotheken und Geräte auswählen, die Sie in der Heimnetzgruppe freigeben möchten. Außerdem wird Ihnen das Kennwort für die Heimnetzgruppe angezeigt. Über Netzwerkorte erfahren Sie mehr in Kapitel 6, »Netzwerkeinstellungen«.

Nachdem Sie diese Schritte durchgeführt haben, sind Sie als lokaler Administrator auf dem frisch installierten Windows 7 angemeldet. An diesem Punkt kann es erforderlich sein, manuell zusätzliche Gerätetreiber zu installieren, die nicht automatisch installiert wurden. Die Konfiguration von Gerätetreibern für Windows 7 beschreibt Kapitel 4, »Verwalten von Geräten und Datenträgern«.


Windows einrichten
Wählen Sie den aktuellen Standort des Computers aus.
Der Computer ist mit einem Netzwerk verbunden. Es werden automatisch die richtigen Netzwerkeinstellungen auf der Grundlage des Netzwerkstandorts angewendet.
Heimnetzwerk
Wenn sich alle Computer dieses Netzwerks bei Ihnen zuhause befinden und Sie sie erkennen, handelt es sich um ein vertrauenswürdiges Heimnetzwerk. Wählen Sie diese Einstellung nicht für öffentliche Plätze aus, z. B. Cafés oder Flughäfen.
Arbeitsplatznetzwerk
Wenn sich alle Computer dieses Netzwerks am Arbeitsplatz befinden und Sie sie erkennen, handelt es sich um ein vertrauenswürdiges Arbeitsplatznetzwerk. Wählen Sie diese Einstellung nicht für öffentliche Plätze aus, z. B. Cafés oder Flughäfen.
Öffentliches Netzwerk
Wenn Sie nicht alle Computer des Netzwerks erkennen (z. B. in einem Café oder an einem Flughafen oder wenn Sie ein mobiles Breitband verwenden), handelt es sich um ein öffentliches Netzwerk, das nicht vertrauenswürdig ist.
Wählen Sie "Öffentliches Netzwerk" aus, wenn Sie sich nicht sicher sind.

Abbildung 1.4 Auswählen des Netzwerktyps

Dual-Boot-Installationen

Dual-Boot-Installationen machen es möglich, auf demselben Computer zwei oder mehr Betriebssysteme nebeneinander zu installieren. Dann können Sie beim Hochfahren des Computers je nach installierten Systemen zum Beispiel zwischen Windows XP und Windows 7 wählen, oder zwischen Windows Vista und Windows 7. Beim Start des Computers wird ein Menü angezeigt, in dem Sie das gewünschte Betriebssystem auswählen können (Abbildung 1.5).

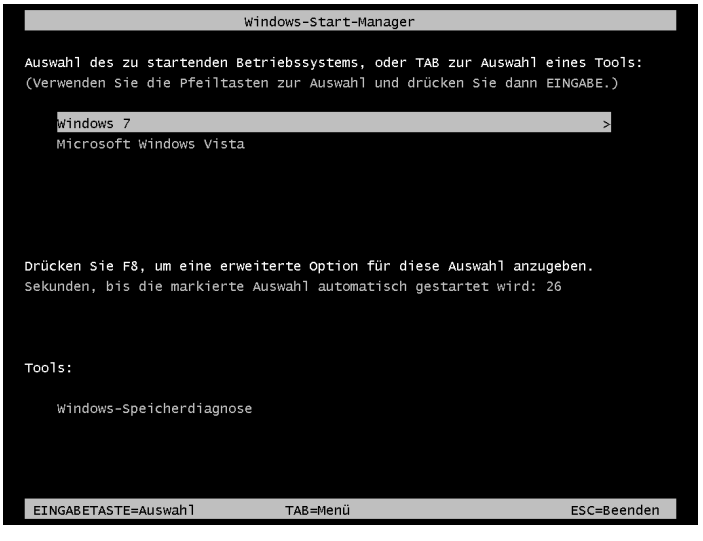

Windows-Start-Manager
Auswahl des zu startenden Betriebssystems, oder TAB zur Auswahl eines Tools:
(Verwenden Sie die Pfeiltasten zur Auswahl und drücken Sie dann EINGABE.)
Windows 7
Microsoft Windows Vista
Drücken Sie F8, um eine erweiterte Option für diese Auswahl anzugeben.
Sekunden, bis die markierte Auswahl automatisch gestartet wird: 26
Tools:
Windows-Speicherdiagnose
EINGABETASTE=Auswahl
TAB=Menü
ESC=Beenden

Abbildung 1.5 Auswählen des zu startenden Betriebssystems

Die Installation von mehreren Betriebssystemen nebeneinander ist heute weniger gebräuchlich als früher, da Virtualisierungsanwendungen wie Microsoft Virtual PC 2007 die Verwendung von älteren Betriebssystemen unter neuen Betriebssystemen ermöglichen. Dual-Boot- oder Multiboot-Lösungen werden heutzutage eher deswegen eingesetzt, weil die Hardware nicht für virtuelle Lösungen ausreicht. Erfüllt ein Computer zum Beispiel nur die Mindestvoraussetzungen für Windows 7, aber Sie müssen gelegentlich noch Programme verwenden, die nur unter Windows XP laufen, kommt eigentlich nur eine Dual-Boot-Lösung in Betracht und keine Virtualisierungslösung, weil der Computer unter Windows 7 nicht über genügend Arbeitsspeicher verfügt, um auch noch einen virtuellen Windows XP-Computer zu starten. In diesem Fall konfigurieren Sie den Computer so, dass der Benutzer wahlweise Windows XP oder Windows 7 starten kann.

Der Schlüssel für eine saubere Dual-Boot-Lösung besteht darin, jedem Betriebssystem eine eigene Partition oder ein eigenes Festplattenlaufwerk zu geben. Für den Fall, dass Sie keine freie Partition oder kein weiteres Festplattenlaufwerk zur Verfügung haben, bieten Windows Vista und Windows 7 ein Tool an, mit dem Sie ein vorhandenes Volume verkleinern können, um in dem frei werdenden Platz ein neues Volume anzulegen. Dieses Tool ist über die Konsole *Datenträgerverwaltung* zugänglich. Um ein Volume zu verkleinern, klicken Sie es in der Konsole *Datenträgerverwaltung* mit der rechten Maustaste an und klicken dann auf *Volume verkleinern*.

Um Windows 7 für eine Dual-Boot-Lösung zu installieren, müssen Sie ein neues Volume mit mindestens 15 GByte anlegen. Auch wenn auf dem zu verkleinernden Volume mehr Speicherplatz frei ist, können Sie das Volume vielleicht nicht genügend verkleinern, weil Windows Vista vielleicht bestimmte Datentypen nicht an einen anderen Ort auf der Festplatte verschieben kann. Windows XP bietet keine Tools, mit denen sich vorhandene Volumes verkleinern lassen. Allerdings sind Produkte von anderen Herstellern erhältlich, die über diese Funktion verfügen.

Wenn Sie einen neuen Computer so einrichten, dass der Benutzer unter mehreren Betriebssystemen auswählen kann, sollten Sie die Betriebssysteme in der Reihenfolge installieren, in der sie erschienen sind. Wollen Sie beispielsweise Windows XP und Windows 7 auf einem neuen Computer nebeneinander verwenden, müssen Sie zuerst Windows XP installieren, bevor Sie Windows 7 installieren. Falls Sie Windows XP erst nach Windows 7 installieren, erkennt das Windows XP-Installationsprogramm die Windows 7-Installation nicht und auf dem Computer kann anschließend nur Windows XP gestartet werden. Es ist dann zwar möglich, den Computer mit der *Systemstartreparatur* von Windows 7 zu reparieren, damit sich beide Betriebssysteme verwenden lassen, aber am einfachsten ist es, die Betriebssysteme in der Reihenfolge zu installieren, in der Microsoft sie veröffentlicht hat.

Um eine Dual-Boot-Konfiguration mit Windows 7 einzurichten, können Sie den Computer entweder vom Windows 7-Installationsmedium starten oder die Installation in der vorhandenen Windows-Version starten. Wenn Sie gefragt werden, ob Sie ein Upgrade oder eine benutzerdefinierte Installation durchführen möchten, wählen Sie die benutzerdefinierte Installation (Abbildung 1.6). Wenn Sie ein Upgrade von Windows XP wählen, wird das Installationsprogramm beendet, weil es nicht möglich ist, Windows XP auf Windows 7 zu aktualisieren. Wenn Sie ein Upgrade von Windows Vista wählen, erfolgt das gewählte Upgrade und Sie können nicht beide Systeme nebeneinander verwenden, weil Windows Vista anschließend nicht mehr vorhanden ist. Wenn Sie diesen Fehler machen, ist es aller-

dings bis zu dem Punkt, an dem Sie sich erfolgreich bei der neuen Windows 7-Installation anmelden, möglich, den Computer in die ursprüngliche Konfiguration zurückzuversetzen.


Windows installieren
Wählen Sie eine Installationsart aus:
Upgrade
Aktualisiert auf eine neuere Version von Windows und behält Dateien, Einstellungen und Programme bei. Die Upgradeoption ist nur verfügbar, wenn eine vorhandene Windows-Version ausgeführt wird. Wir empfehlen, eine Sicherung Ihrer Dateien zu erstellen, bevor Sie fortfahren.
Benutzerdefiniert (erweitert)
Installiert eine neue Windows-Kopie. Bei Verwendung dieser Option werden Dateien, Einstellungen und Programme nicht beibehalten. Die Option, Änderungen an Datenträgern und Partitionen vorzunehmen, ist verfügbar, wenn Sie den Computer über den Installationsdatenträger starten. Wir empfehlen, eine Sicherung Ihrer Dateien zu erstellen, bevor Sie fortfahren.
Entscheidungshilfe

Abbildung 1.6 Zur Einrichtung eines Dual-Boot-Systems wählen Sie die benutzerdefinierte Installation

Der Installationsverlauf bei der Einrichtung eines Dual-Boot-Systems ist derselbe wie bei der Neuinstallation. Die Hauptschwierigkeit ist es, an dem Punkt, an dem Sie angeben müssen, wo das Betriebssystem installiert werden soll, die richtige Festplatte oder das richtige Volume anzugeben. Wenn Sie versehentlich das Volume oder die Festplatte angeben, auf der das andere Betriebssystem installiert ist, das Sie neben Windows 7 verwenden möchten, kann es damit enden, dass dieses Volume gelöscht wird und eine Neuinstallation von Windows 7 erfolgt. Nach dem Abschluss können Sie das gewünschte Betriebssystem beim Hochfahren des Computers auswählen, wobei Windows 7 das Standardbetriebssystem ist. Wie man das Standardbetriebssystem konfiguriert, erfahren Sie weiter unten in dieser Lektion.

Dual-Boot und virtuelle Festplatten

Die Ausnahme von der Regel, dass Sie für jedes Betriebssystem eine separate Partition brauchen, ist der Start eines Betriebssystems aus einer VHD-Datei. Sie können die Editionen Windows 7 Enterprise und Ultimate sowie Windows Server 2008 R2 in VHD-Dateien installieren und aus diesen Dateien heraus starten. Der Start des Computers aus einer VHD-Datei heraus ist aber nur auf Computern möglich, auf denen die Startumgebung von Windows 7 oder Windows Server 2008 R2 verwendet wird. Das bedeutet, dass Sie einen Windows XP- oder Windows Vista-Computer nicht für das Dual-Boot mit Windows 7 einrichten können, wenn Windows 7 in einer VHD-Datei installiert wird. Allerdings ist es möglich, ein Triple-Boot mit Windows 7 in einer VHD einzurichten, wenn auf dem Computer bereits ein Dual-Boot mit Windows 7 und einer älteren Windows-Version möglich ist. Das liegt daran, dass auf dem Computer, für den Sie ein Dual-Boot mit Windows 7 eingerichtet haben, die

Windows 7-Startumgebung verwendet wird. Wie man Windows 7 in einer VHD-Datei installiert, erfahren Sie in Kapitel 2.

Konfigurieren des Standardbetriebssystems

Wenn Sie einen Computer für Dual-Boot konfigurieren, wird eines der Betriebssysteme als Standardbetriebssystem ausgewählt. Das bedeutet, dass der Computer mit diesem Betriebssystem gestartet wird, sofern der Benutzer kein anderes auswählt. Welches Betriebssystem das Standardbetriebssystem ist, können Sie in der grafischen Benutzeroberfläche von Windows ändern:

1. Öffnen Sie die Systemsteuerung im *Start*-Menü. Wählen Sie in der Dropdownliste *Anzeige* den Eintrag *Kleine Symbole*.
2. Klicken Sie auf *System* und dann auf *Erweiterte Systemeinstellungen*. Dadurch öffnet sich das Dialogfeld *Systemeigenschaften*.
3. Klicken Sie auf der Registerkarte *Erweitert* im Abschnitt *Starten und Wiederherstellen* auf *Einstellungen*. Dadurch öffnet sich das Dialogfeld *Starten und Wiederherstellen* (Abbildung 1.7).

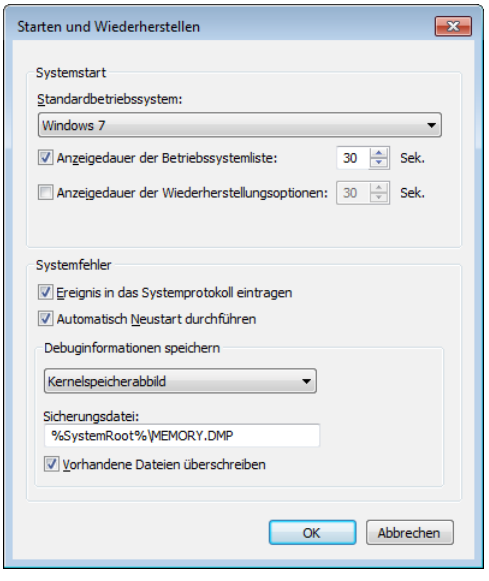


Abbildung 1.7 Auswählen des Standardbetriebssystems

4. Wählen Sie in der Dropdownliste *Standardbetriebssystem* das Betriebssystem aus, das standardmäßig für den Start des Computers verwendet werden soll.

Die Konfiguration des Standardbetriebssystems mit dem Befehlszeilenprogramm *Bcdedit.exe* ist etwas komplizierter:

1. Öffnen Sie eine administrative Eingabeaufforderung, indem Sie den Eintrag *Eingabeaufforderung* im Menü *Zubehör* des *Start*-Menüs mit der rechten Maustaste anklicken und *Als Administrator ausführen* wählen. Klicken Sie in der Bestätigungsaufforderung der Benutzerkontensteuerung auf *Ja*.

2. Geben Sie den Befehl **bcdedit /enum** ein, um eine Liste der aktuellen Startmenüeinträge anzuzeigen. Die Liste wird so ähnlich aussehen wie in Abbildung 1.8.

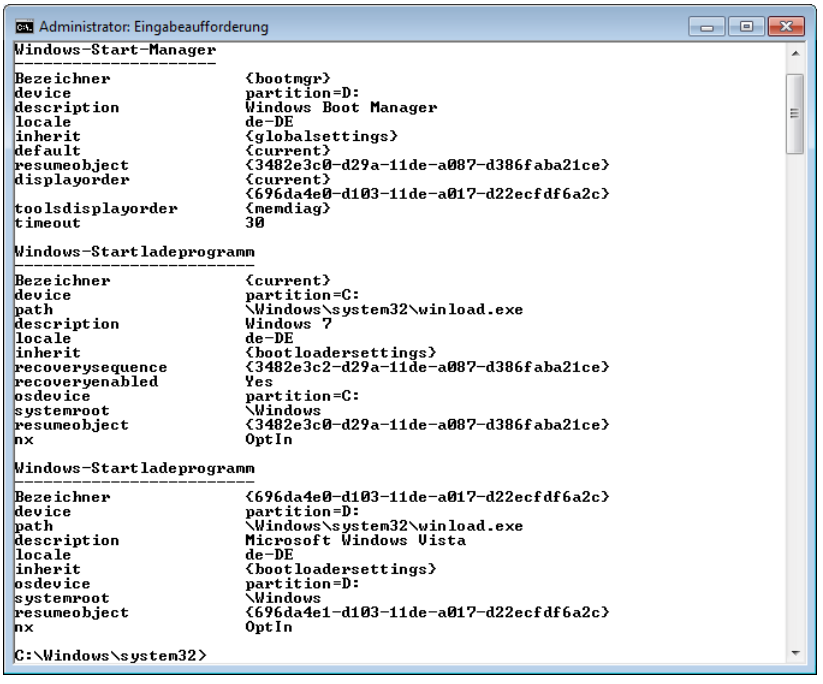


Abbildung 1.8 Bearbeiten des Startmenüs mit BCDEdit

3. Um den Standardeintrag zu ändern, verwenden Sie den Befehl `bcdedit /default` und geben die entsprechende Kennung an. In Abbildung 1.8 wäre dies {696da4e1-d103-11de-a017-d22ecfdf6a2c}.



Hinweis Dual-Boot mit anderen Betriebssystemen

Es ist auch möglich, einen Computer für den Dual-Boot mit Windows 7 und einem anderen PC-Betriebssystem wie Linux einzurichten, oder mit speziellen Hilfsprogrammen wie Mac OS X auf einem Macintosh. Es ist aber sehr unwahrscheinlich, dass diese Konfigurationen in der Prüfung 70-680 abgefragt werden.

Übung Durchführen einer Neuinstallation

Wenn Sie auf einem Computer, der noch nicht über ein Betriebssystem verfügt, ein Betriebssystem installieren, führen Sie eine Neuinstallation durch. Eine Neuinstallation hat den Vorteil, dass Sie sich nicht um den Erhalt von Daten kümmern müssen, weil es auf dem Computer noch keine erhaltenswerten Daten gibt. Diese Art von Installation führen Sie auf Computern durch, die frisch vom Hersteller eingetroffen sind, oder auf einem Computer, dessen Festplatte Sie durch eine neue Festplatte ersetzt haben und dessen Betriebssystem Sie nicht aus einer vorhandenen Sicherung wiederherstellen möchten.

Übung Windows 7-Installation

In dieser Übung installieren Sie Windows 7 auf einem Computer, der noch nicht über ein Betriebssystem verfügt. Die Beschreibung geht zwar von einer DVD als Installationsquelle aus, aber Sie können für die Installation auch ein entsprechend vorbereitetes USB-Speichergerät verwenden, von dem Sie den Computer starten. Bevor Sie die Übung beginnen, stellen Sie das BIOS des Computers so ein, dass er sich von dem vorgesehenen Gerät starten lässt.

1. Legen Sie das Windows 7-Installationsmedium in das DVD-Laufwerk des Computers ein und schalten Sie den Computer ein. Sie werden wahrscheinlich aufgefordert, eine Taste zu drücken, um den Computer von DVD zu starten.
2. Wählen Sie auf der ersten Seite des Windows-Installationsassistenten die Sprache, die Sie für die Installation verwenden möchten, das gewünschte Datums- und Zeitformat sowie die gewünschte Tastatur oder Eingabemethode (Abbildung 1.9). Klicken Sie auf *Weiter*.


Windows installieren
Windows 7
Installationssprache: Deutsch
Uhrzeit und Währungsformat: Deutsch (Deutschland)
Tastatur oder Eingabemethode: Deutsch
Geben Sie Ihre Sprache und andere Einstellungen ein und klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
Copyright © 2009 Microsoft Corporation. Alle Rechte vorbehalten.
Weiter

Abbildung 1.9 Auswählen der Installationssprache

3. Klicken Sie auf *Jetzt installieren*. Überprüfen Sie die Lizenzbedingungen. Wenn Sie einverstanden sind, markieren Sie das Kontrollkästchen *Ich akzeptiere die Lizenzbedingungen*. Klicken Sie auf *Weiter*.
4. Auf der Seite *Wählen Sie eine Installationsart aus* klicken Sie auf *Benutzerdefiniert (erweitert)*. Dadurch können Sie eine neue Kopie von Windows 7 installieren.
5. Wählen Sie auf der Seite *Wo möchten Sie Windows installieren?* ein Festplattenlaufwerk aus, das über mindestens 16 GByte freien Speicherplatz verfügt (Abbildung 1.10). Falls keine Festplatte angezeigt wird, müssen Sie vielleicht auf *Treiber laden* klicken und einen Treiber für die Festplatte laden. Da es sich um eine Neuinstallation handelt, sollten auf den Festplatten, die in diesem Dialogfeld angezeigt werden, noch keine formatierten Volumes vorhanden sein. Klicken Sie auf *Weiter*.

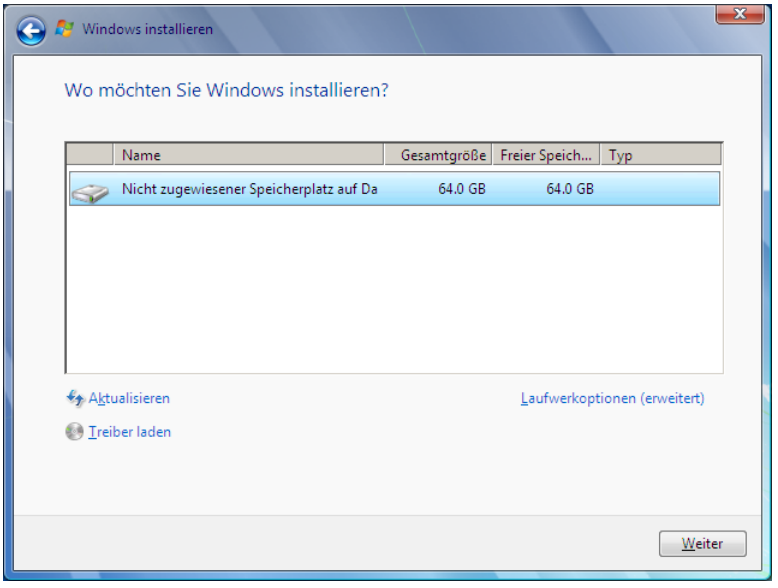


Abbildung 1.10 Auswählen des Festplattenlaufwerks, auf dem Windows 7 installiert werden soll

6. Die Installation beginnt. Je nach der Geschwindigkeit des Computers, auf dem Sie Windows 7 installieren, kann dies einige Zeit in Anspruch nehmen. Während der Installation wird der Computer mehrere Male neu gestartet.
7. Wenn Sie die in Abbildung 1.11 gezeigte Seite sehen, geben Sie den Benutzernamen **Kim_Akers** und den Computernamen **Canberra** ein und klicken dann auf *Weiter*.

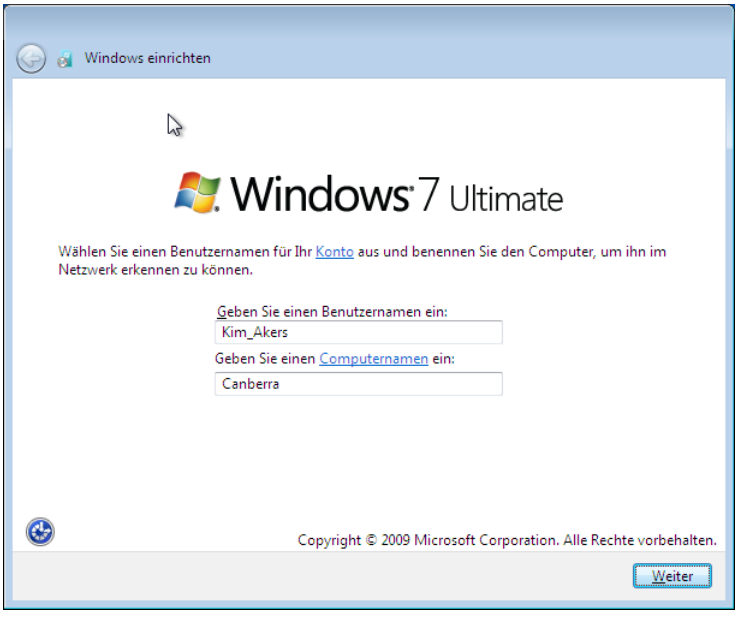

Windows einrichten
Windows 7 Ultimate
Wählen Sie einen Benutzernamen für Ihr Konto aus und benennen Sie den Computer, um ihn im Netzwerk erkennen zu können.
Geben Sie einen Benutzernamen ein:
Kim_Akers
Geben Sie einen Computernamen ein:
Canberra
Copyright © 2009 Microsoft Corporation. Alle Rechte vorbehalten.
Weiter

Abbildung 1.11 Eingabe von Benutzer- und Computername

8. Geben Sie auf der Seite *Kennwort für das eigene Konto festlegen* zweimal das Kennwort **P@ssw0rd** ein. Als Kennworthinweis könnten Sie zum Beispiel die Seitennummer dieses Buchs eingeben. Klicken Sie auf *Weiter*.
9. Geben Sie auf der Seite *Geben Sie den Product Key ein* Ihren Product Key ein, aber löschen Sie das Kontrollkästchen *Windows automatisch aktivieren, wenn eine Internetverbindung besteht*. Klicken Sie auf *Weiter*.
10. Klicken Sie auf der Seite *Schützen Sie Ihren Computer, und verbessern Sie Windows automatisch* auf *Später erneut nachfragen*.
11. Konfigurieren Sie auf der Seite *Überprüfen Sie die Zeit- und Datumseinstellungen* die Zeitzone, aktivieren Sie bei Bedarf die automatische Umstellung auf die Sommerzeit und überprüfen Sie das Datum und die Uhrzeit (Abbildung 1.12). Klicken Sie dann auf *Weiter*.

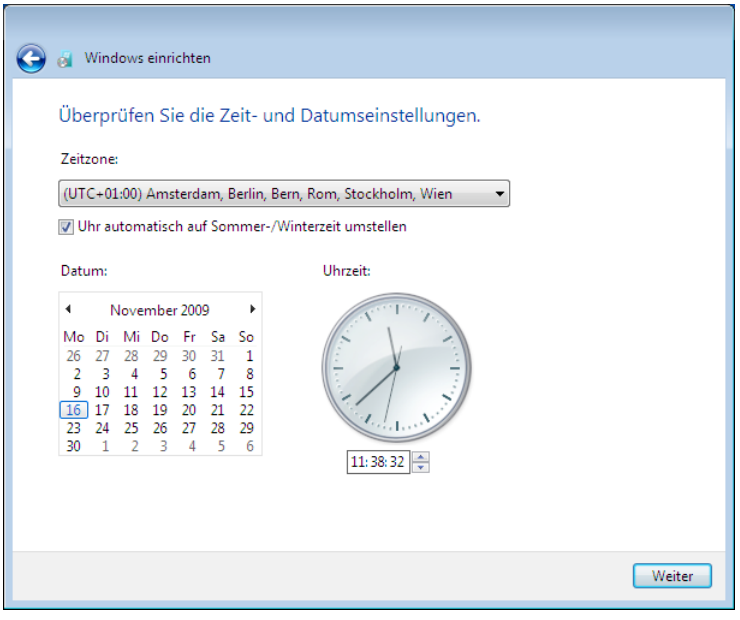

Windows einrichten
Überprüfen Sie die Zeit- und Datumseinstellungen.
Zeitzone:
(UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
Uhr automatisch auf Sommer-/Winterzeit umstellen
Datum:
Uhrzeit:
November 2009
Mo Di Mi Do Fr Sa So
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 1 2 3 4 5 6
11:38:32
Weiter

Abbildung 1.12 Zeit- und Datumseinstellungen

12. Klicken Sie auf der Seite *Wählen Sie den aktuellen Standort des Computers aus* auf *Heimnetzwerk*. Das Installationsprogramm schließt die Installation ab. Anschließend sind Sie als lokaler Administrator auf dem Computer angemeldet.
13. Sofern Sie nun gefragt werden, ob Sie eine Heimnetzgruppe erstellen möchten, wählen Sie alle Bibliotheken aus und notieren sich das Kennwort für die Heimnetzgruppe. Ist dies nicht der Fall, klicken Sie auf das *Start*-Menü, dann auf *Systemsteuerung* und schließlich unter *Netzwerk und Internet* auf *Heimnetzgruppen- und Freigabeoptionen auswählen*. Klicken Sie dann auf der Seite *Für andere Heimcomputer unter Windows 7 freigeben* auf *Was ist eine Netzwerkadresse*. Wählen Sie als Netzwerkort *Heimnetzwerk*. Wählen Sie im Dialogfeld *Heimnetzgruppe erstellen* alle Objekte aus (Abbildung 1.13) und klicken Sie auf *Weiter*. Notieren Sie sich das Kennwort, das auf der nächsten Seite angezeigt wird, und klicken Sie auf *Fertig stellen*. Schließen Sie die

Systemsteuerung. Heimnetzwerke und Heimnetzgruppen werden in Kapitel 8 ausführlicher besprochen. Nach diesem Schritt ist die Installation abgeschlossen. Fahren Sie den Computer herunter.

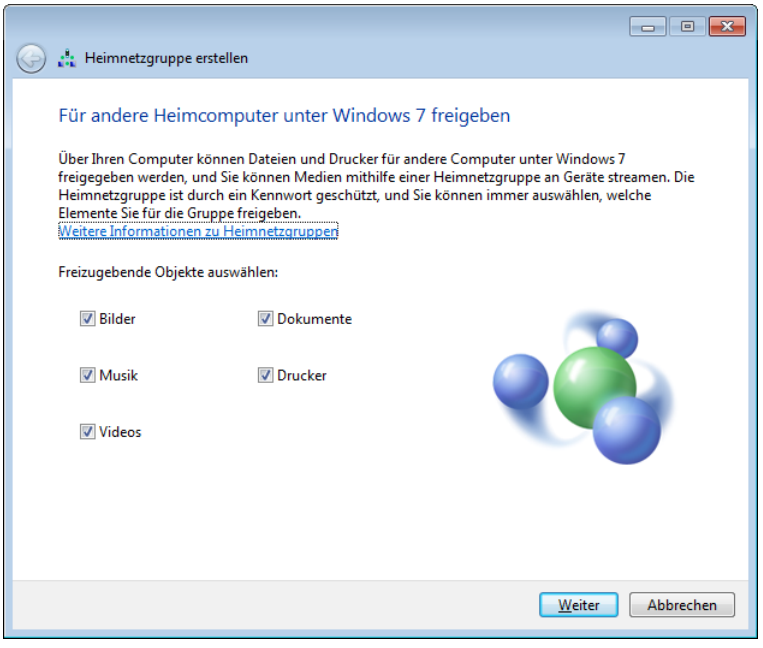

Heimnetzgruppe erstellen
Für andere Heimcomputer unter Windows 7 freigeben
Über Ihren Computer können Dateien und Drucker für andere Computer unter Windows 7 freigegeben werden, und Sie können Medien mithilfe einer Heimnetzgruppe an Geräte streamen. Die Heimnetzgruppe ist durch ein Kennwort geschützt, und Sie können immer auswählen, welche Elemente Sie für die Gruppe freigeben.
Weitere Informationen zu Heimnetzgruppen
Freizugebende Objekte auswählen:
Bilder
Dokumente
Musik
Drucker
Videos
Weiter
Abbrechen

Abbildung 1.13 Erstellen einer Heimnetzgruppe

Zusammenfassung der Lektion

- Windows 7 ist in sechs verschiedenen Editionen erhältlich. Die Editionen unterscheiden sich im Funktionsumfang. Nur die Editionen Professional, Enterprise und Ultimate lassen sich zu Domänen hinzufügen. Nur die Editionen Enterprise und Ultimate enthalten Unternehmensfunktionen wie BitLocker, AppLocker, DirectAccess und BranchCache.
- Von Windows 7 gibt es zwei verschiedene Versionen. Die 32-Bit-Version wird auch x86-Version genannt, die 64-Bit-Version auch x64-Version. Die 32-Bit-Version unterstützt maximal 4 GByte Arbeitsspeicher. Die x64-Versiont unterstützt je nach Edition 8 bis 128 GByte.
- Die Editionen Windows 7 Home Basic und Starter setzen einen x86- oder x64-Prozessor mit einer Taktfrequenz von 1 GHz, 512 MByte Arbeitsspeicher, einem Festplattenlaufwerk mit 20 GByte Speicherplatz und einer Grafikkarte mit 32 MByte Grafikspeicher voraus, die DirectX9 unterstützt.
- Die Editionen Windows 7 Home Premium, Professional, Enterprise und Ultimate setzen einen x86- oder x64-Prozessor mit einer Taktfrequenz von 1 GHz, 1 GByte Arbeitsspeicher, einem Festplattenlaufwerk mit 20 GByte Speicherplatz und einer Grafikkarte mit 128 MByte Grafikspeicher voraus, die über einen WDDM-Treiber verfügt, 32 Bit pro Pixel verwenden kann und Pixel Shader 2.0 sowie DirectX9 unterstützt.

- Windows 7 kann von einem DVD-Laufwerk, einem USB-Speichergerät, einer Netzwerkfreigabe oder von einem Windows-Bereitstellungsdiensteserver installiert werden. DVD-Laufwerke und USB-Speichergeräte eignen sich gut, wenn nur wenige Computer bereitgestellt werden müssen. Für große Stückzahlen ist WDS besser geeignet, während sich die Netzwerkfreigabe auch in Umgebungen einsetzen lässt, die kein WDS bieten.
- Windows 7 kann in einer Dual-Boot-Konfiguration mit Windows XP, Windows Vista und Windows 7 kombiniert werden. Von VHD kann ein Computer nur dann Windows 7 starten, wenn er über eine Windows 7- oder Windows Server 2008 R2-Startumgebung verfügt.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Installieren von Windows 7«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Mit welchem Hilfsprogramm können Sie ein USB-Speichergerät so vorbereiten, dass ein Laptop, der nicht über ein DVD-Laufwerk verfügt, von diesem Gerät starten und Windows 7 installiert werden kann?
   A. *LoadState.exe*
   B. *ScanState.exe*
   C. Diskpart
   D. BCDEdit
2. Sie möchten einen neuen Computer für Softwarekompatibilitätstests bereitstellen. Dieser Computer muss mit den Betriebssystemen Windows 7, Windows XP und Windows Vista gestartet werden können. In welcher Reihenfolge sollten Sie die Betriebssysteme installieren, damit sich diese Anforderung ohne zusätzliche Bearbeitung der Starteinträge mit BCDEdit erfüllen lässt?
   A. Windows 7, Windows XP und dann Windows Vista
   B. Windows Vista, Windows 7 und dann Windows XP
   C. Windows XP, Windows 7 und dann Windows Vista
   D. Windows XP, Windows Vista und dann Windows 7
3. Mit welchen der folgenden Editionen und Versionen von Windows 7 können Sie die Hardwareressourcen eines Computers nutzen, der über 16 GByte Arbeitsspeicher verfügt? (Wählen Sie alle zutreffenden Antworten.)
   A. Windows 7 Ultimate x86
   B. Windows 7 Professional x64
   C. Windows 7 Enterprise x86
   D. Windows 7 Home Premium x64

4. Sie möchten mit WDS eine Netzwerkinstallation von Windows 7 durchführen. Über welche Hardwaregeräte muss der Computer verfügen, wenn Sie ihn nicht mit einem WDS-Suchabbild starten?
   A. Ein DVD-Laufwerk
   B. Eine PXE-konforme Netzwerkkarte
   C. Einen USB 2.0-Anschluss
   D. Einen HDMI-Anschluss
5. Über wie viele Volumes muss ein Computer, auf dem Windows XP ausgeführt wird, mindestens verfügen, damit eine Dual-Port-Konfiguration mit Windows 7 eingerichtet werden kann?
   A. 1
   B. 2
   C. 3
   D. 4

Lektion 2: Aktualisieren auf Windows 7

Die meisten großen Organisationen verwenden zwar Systemabbilder, um ein Betriebssystem schnell auf neuen Computern installieren und Einstellungen und Anwendungen konfigurieren zu können, aber die meisten kleineren Organisationen betreiben die Verwaltung der Desktopcomputer auf eine etwas riskantere Weise. Anwendungen werden meistens nach einem kurzfristig festgestellten Bedarf eingekauft und installiert, und in vielen Organisationen gibt es keine zwei Computer, auf denen dieselben Anwendungen installiert sind. Das kann die Einführung eines neuen Betriebssystems ziemlich kompliziert machen. Wenn Sie Neuinstallationen durchführen, müssen Sie dafür sorgen, dass Sie genau die Anwendungen installieren können, die die Benutzer gewohnt sind. Die Aktualisierung eines Betriebssystems auf eine neue Version bietet den großen Vorteil, dass alle Benutzerdaten und Anwendungen, die auf dem alten Betriebssystem vorhanden waren, auch auf dem aktualisierten Betriebssystem vorhanden sind. In dieser Lektion erfahren Sie etwas über die Bedingungen, unter denen Sie ein Betriebssystem auf Windows 7 aktualisieren und dabei die vorhandenen Anwendungen und Daten beibehalten können.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Computer von Windows Vista auf Windows 7 aktualisieren
- Computer von Windows XP auf Windows 7 migrieren
- Computer von einer vorhandenen Windows 7-Edition auf eine andere Edition von Windows 7 aktualisieren

Veranschlagte Zeit für diese Lektion: 70 Minuten

Aktualisieren von Windows 7-Editionen

Manchmal ist es erforderlich, einen Computer von einer vorhandenen Windows 7-Edition auf eine andere umzustellen. Denken Sie zum Beispiel an eine kleine Firma, die einige Laptops mit vorinstalliertem Windows 7 Home Basic angeschafft hat, aber BitLocker verwenden und die Computer zu Domänen hinzufügen möchte. Statt die Festplatten alle zu löschen und eine andere Windows 7-Version zu installieren, ist es auch möglich, diese Computer auf eine Windows 7-Edition zu aktualisieren, die über die gewünschten Leistungsmerkmale verfügt.

Eine Aktualisierung auf eine andere Windows 7-Edition hat gegenüber einer Neuinstallation mit der gewünschten Edition einige Vorteile. Der erste ist ein Kostenvorteil. Die Aktualisierung einer vorhandenen auf die gewünschte Edition ist billiger als der Neukauf einer neuen Betriebssystemlizenz. Eine Aktualisierung von Windows 7 Home Basic auf Windows 7 Ultimate ist zum Beispiel billiger als eine neue Windows 7 Ultimate-Lizenz. Der zweite Vorteil liegt darin, dass alle Anwendungen und Daten erhalten bleiben, die bereits auf dem betreffenden Computer vorhanden sind.

Wie Sie in Lektion 1 erfahren haben, ist jede Windows 7-Edition eine Obermenge der jeweils niedrigeren Edition. Windows 7 Professional enthält alle Funktionen von Windows Home Premium und einige zusätzliche Funktionen. Windows 7 Ultimate enthält alle Funktionen von Windows 7 Professional und wiederum einige zusätzliche Funktionen.

Windows 7 ermöglicht die Aktualisierung von einer Edition auf eine andere, solange der Funktionsumfang der gewünschten Edition größer ist. Sie können zum Beispiel von Home

Premium auf die Editionen Professional, Enterprise oder Ultimate aktualisieren, aber nicht von Ultimate auf die Editionen Home Premium oder Professional.

Es ist zwar möglich, eine Aktualisierung auf höhere Editionen von Windows 7 durchzuführen, aber ein Wechsel zwischen den Versionen von Windows 7 ist nicht möglich. Sie können eine x86-Version nicht auf eine x64-Version aktualisieren. Ebenso wenig können Sie eine x64-Version auf eine x86-Version umstellen. Nehmen wir zum Beispiel an, ein Entwickler aus Ihrer Organisation verfügt über einen Computer mit 4 GByte Arbeitsspeicher und der x86-Version von Windows 7 Enterprise. Dieser Entwickler führt viele Anwendungskompatibilitätstests durch und verwendet dafür virtuelle Computer, für die er wiederum mehr Arbeitsspeicher braucht. Die x86-Version von Windows 7 Enterprise unterstützt maximal 4 GByte Arbeitsspeicher, die x64-Version von Windows 7 Enterprise dagegen bis zu 128 GByte. Allerdings ist es nicht möglich, die x86-Version von Windows 7 Enterprise auf die x64-Version von Windows 7 zu aktualisieren. Daher wird es bei der Umstellung erforderlich, eine Migration auf demselben Computer (Wipe-and-Load) durchzuführen. Dazu müssen die Daten des Entwicklers gesichert werden, bevor eine Neuinstallation des x64-Betriebssystems erfolgt und die Daten wieder auf den aktualisierten Computer importiert werden. Als Alternative bietet es sich an, eine Dual-Boot-Konfiguration mit einer x86- und einer x64-Edition von Windows 7 einzurichten, was durch die Möglichkeit des Starts von VHD in den Editionen Enterprise und Ultimate noch erleichtert wird. Allerdings ist es trotzdem noch erforderlich, die Daten vom alten Betriebssystem auf das neue Betriebssystem zu übernehmen. Die Migration wird in Lektion 3, »Verwalten von Benutzerprofilen«, ausführlicher besprochen.

Zur Aktualisierung von einer Windows 7-Edition auf eine andere können Sie eine der beiden folgenden Methoden verwenden:

- **Aktualisieren mit dem Installationsmedium** Die Aktualisierung mit dem Medium lässt sich mit der Aktualisierung von Windows Vista vergleichen. Sie erwerben einen Product Key für die Edition, auf die Sie die Aktualisierung durchführen wollen, und verwenden für die Aktualisierung dann das Windows 7-Installationsmedium. Diese Methode eignet sich am besten für Organisationen, in denen eine große Zahl von Aktualisierungen erforderlich ist.
- **Windows Anytime Upgrade** Mit Windows Anytime Upgrade (Abbildung 1.14) können Sie eine Aktualisierung über das Internet erwerben und die zusätzlichen Funktionen automatisch freischalten. Diese Aktualisierungsmethode eignet sich eher für Privatanwender und Anwender in kleinen Firmen, in denen nur wenige Aktualisierungen erforderlich sind.

Aktualisieren von Windows Vista

Sie können Computer, auf denen Windows Vista verwendet wird, auf Windows 7 aktualisieren. Wenn Sie eine Aktualisierung von Windows Vista auf Windows 7 durchführen, sind alle Dokumente, Einstellungen, Anwendungen und Benutzerkonten, die es auf dem Windows Vista-Computer gibt, nach der Aktualisierung noch vorhanden. Der Vorteil einer Aktualisierung besteht darin, dass die aktuelle Anwendungskonfiguration erhalten bleibt. Wenn Sie eine Migration durchführen, müssen Sie die Anwendungen des Benutzers auf dem neuen Computer neu installieren. Wie bereits erwähnt, kann dies in Organisationen, die über die auf den einzelnen Computern installierten Anwendungen nicht so genau Buch führen, durchaus ein Problem werden.

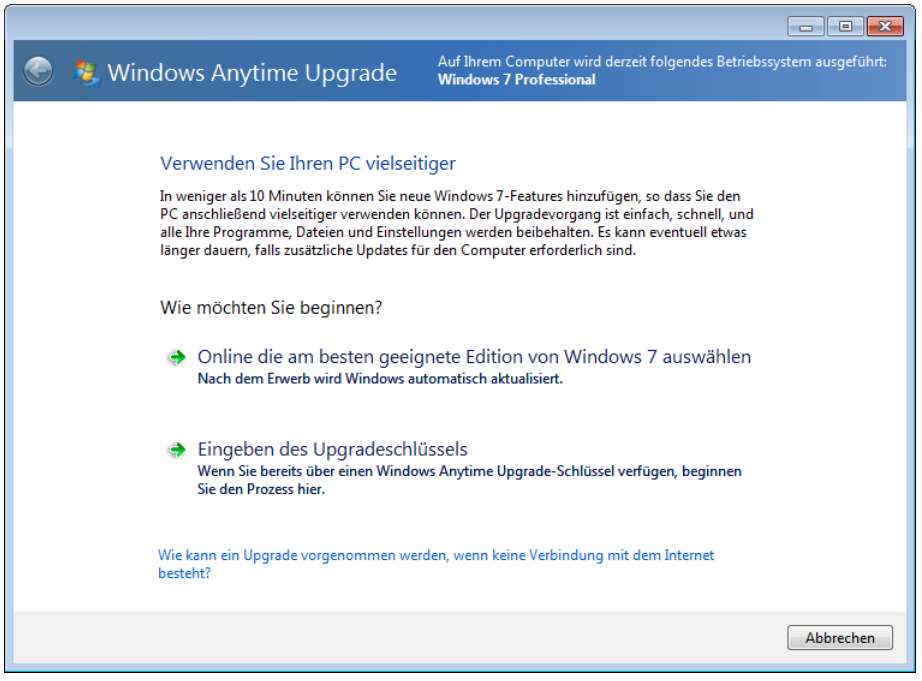

Windows Anytime Upgrade
Auf Ihrem Computer wird derzeit folgendes Betriebssystem ausgeführt:
Windows 7 Professional
Verwenden Sie Ihren PC vielseitiger
In weniger als 10 Minuten können Sie neue Windows 7-Features hinzufügen, so dass Sie den PC anschließend vielseitiger verwenden können. Der Upgradevorgang ist einfach, schnell, und alle Ihre Programme, Dateien und Einstellungen werden beibehalten. Es kann eventuell etwas länger dauern, falls zusätzliche Updates für den Computer erforderlich sind.
Wie möchten Sie beginnen?
Online die am besten geeignete Edition von Windows 7 auswählen
Nach dem Erwerb wird Windows automatisch aktualisiert.
Eingeben des Upgradeschlüssels
Wenn Sie bereits über einen Windows Anytime Upgrade-Schlüssel verfügen, beginnen Sie den Prozess hier.
Wie kann ein Upgrade vorgenommen werden, wenn keine Verbindung mit dem Internet besteht?
Abbrechen

Abbildung 1.14 Windows Anytime Upgrade

Vor dem Versuch einer Aktualisierung von Windows Vista auf Windows 7 sollten Sie den Windows 7 Upgrade Advisor verwenden, den Sie von der Microsoft-Website herunterladen können. Er überprüft, ob sich die Hardware- und Softwarekonfiguration eines Windows Vista-Computers für Windows 7 eignet. Sorgen Sie vor dem Start des Windows 7 Upgrade Advisors dafür, dass auch die externe Hardware wie Drucker, Scanner und Fotoapparate, die Sie unter Windows 7 verwenden möchten, an den Computer angeschlossen und eingeschaltet ist. Der Upgrade Advisor erstellt einen Bericht, in dem er Sie darüber informiert, mit welchen Anwendungen und Geräten es unter Windows 7 höchstwahrscheinlich zu Problemen kommt. Ein ähnlicher Kompatibilitätsbericht wird auch während der Aktualisierung erstellt, aber die Version, die der Windows 7 Upgrade Advisor erstellt, ist wahrscheinlich aktueller.



Weitere Informationen Windows 7 Upgrade Advisor

Den Windows 7 Upgrade Advisor erhalten Sie im Microsoft Download Center unter *http://www.microsoft.com/downloads/search.aspx?displaylang=de.*



Hinweis Verwenden Sie eine Suchmaschine

Eine andere Möglichkeit zur Überprüfung, ob ein bestimmtes Gerät oder eine bestimmte Anwendung zu Windows 7 kompatibel ist, ist die Verwendung einer Suchmaschine. Sehr wahrscheinlich hat vor Ihnen schon jemand versucht, die Geräte oder Anwendungen, an denen Sie interessiert sind, unter Windows 7 zu verwenden. Falls sich Probleme ergeben haben, hat vermutlich schon jemand in einem Forum, einem Blog oder irgendwo anders im World Wide Web darüber geschrieben.

Windows Vista und Windows 7 stellen dieselben Anforderungen an die Hardware. Das bedeutet, dass Sie bei einem Windows Vista-Computer normalerweise weder den Arbeitsspeicher noch den Prozessor austauschen müssen, um Windows 7 verwenden zu können. Allerdings müssen auf dem Windows Vista-Volume für die Aktualisierung mindestens 10 GByte Speicherplatz frei sein. Berücksichtigen Sie vor und während der Aktualisierung von Windows Vista auf Windows 7 folgende Punkte:

- Führen Sie vor der Aktualisierung eine vollständige Sicherung des Windows Vista-Computers durch, dann können Sie den Computer wiederherstellen, falls die Aktualisierung scheitern sollte.
- Sorgen Sie dafür, dass auf dem Windows Vista-Computer Service Pack 1 oder höher installiert ist, bevor Sie mit der Aktualisierung auf Windows 7 beginnen.
- Sorgen Sie vor der Aktualisierung dafür, dass Sie über den Windows 7-Product Key verfügen.
- Bei einer Aktualisierung können Sie nicht die Prozessorarchitektur wechseln. Eine x86-Version von Windows Vista lässt sich nicht auf eine x64-Version von Windows 7 aktualisieren und eine x64-Version von Windows Vista nicht auf eine x86-Version von Windows 7.
- Eine Aktualisierung ist nur auf eine gleichwertige oder höhere Edition von Windows 7 möglich. Sie können Windows Vista Home Premium auf Windows 7 Home Premium, Professional, Enterprise oder Ultimate aktualisieren, aber nicht auf Windows 7 Starter. Windows 7 Professional entspricht in diesem Sinne Windows Vista Business.
- Sorgen Sie dafür, dass auf dem Windows Vista-Volume mindestens 10 GByte Speicherplatz frei sind, bevor Sie mit der Aktualisierung beginnen.

In der Übung am Ende dieser Lektion führen Sie eine Aktualisierung von Windows Vista auf Windows 7 durch.

Rückgängigmachen einer fehlgeschlagenen Aktualisierung

Eine Windows 7-Aktualisierung wird automatisch rückgängig gemacht, falls sich während der Installation Probleme ergeben. Bis zu dem Punkt, an dem eine erfolgreiche Anmeldung erfolgt, können Sie die Aktualisierung auch manuell rückgängig machen. Sollte also ein Problem mit einem Treiber eine erfolgreiche Anmeldung verhindern, können Sie die Aktualisierung rückgängig machen und wieder mit der vorhandenen Windows Vista-Installation arbeiten. Nach einer erfolgreichen Anmeldung unter Windows 7 ist eine Rückführung auf Windows Vista allerdings nur noch durch eine Neuinstallation oder durch eine Wiederherstellung aus einer Sicherung möglich.

Schnelltest

- Unter welchen Bedingungen ist eine Aktualisierung von Windows Vista auf Windows 7 nicht möglich?

Antwort zum Schnelltest

- Sie können keine x86-Version von Windows Vista auf eine x64-Version von Windows 7 aktualisieren und keine x64-Version von Windows Vista auf eine x86-Version von Windows 7. Außerdem lassen sich bestimmte Editionen von Windows Vista nicht auf bestimmte Editionen von Windows 7 aktualisieren.

Migrieren von Windows XP

Windows XP lässt sich nicht direkt auf Windows 7 aktualisieren. Wenn Sie es trotzdem versuchen, erscheint eine Fehlermeldung wie in Abbildung 1.15. Für die Umstellung von Windows XP auf Windows 7 bietet sich aber eine Migration an.

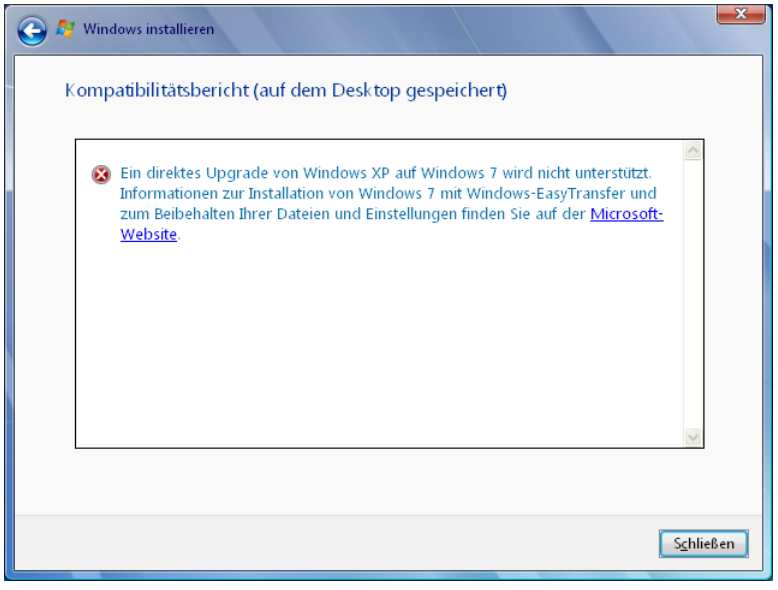

Windows installieren
Kompatibilitätsbericht (auf dem Desktop gespeichert)
Ein direktes Upgrade von Windows XP auf Windows 7 wird nicht unterstützt. Informationen zur Installation von Windows 7 mit Windows-EasyTransfer und zum Beibehalten Ihrer Dateien und Einstellungen finden Sie auf der Microsoft-Website.
Schließen

Abbildung 1.15 Kein direktes Upgrade von Windows XP auf Windows 7

Es gibt zwei Grundszenarien für Migrationen von Benutzerprofildaten: die Migration auf einen anderen Computer (*Side-by-Side-Migration*) und die Migration auf denselben Computer (*Wipe-and-Load-Migration*). Welche Variante sinnvoll ist, hängt hauptsächlich von der Hardware des Quellcomputers ab. Wenn sich die Hardware des Quellcomputers für Windows 7 eignet und Sie keine Dual-Boot-Konfiguration einrichten möchten, können Sie eine Migration auf denselben Computer durchführen. Reicht die Hardware des Quellcomputers nicht für Windows 7 aus, müssen Sie eine Migration auf einen anderen Computer durchführen. Eine Migration auf einen anderen Computer ist auch erforderlich, wenn Sie eine Dual-Boot-Konfiguration einrichten möchten, weil dies die einzige Möglichkeit ist, die Anwendungsdaten von der Windows XP-Partition auf die Windows 7-Partition zu übertragen.

Side-by-Side-Migrationen

Migrationen auf einen anderen Computer sind dann sinnvoll, wenn Sie Benutzerdaten von einem Computer auf einen anderen Computer übertragen möchten. Je nach der Migrationsmethode kann es erforderlich werden, dass beide Computer während der Migration eingeschaltet sind, beispielsweise für eine direkte Übertragung über das Netzwerk oder mit einem Spezialkabel. Der Vorteil einer Migration auf einen anderen Computer liegt darin, dass alle Daten auf dem Quellcomputer erhalten bleiben und auch noch verfügbar sind, wenn die Migration auf den Zielcomputer abgeschlossen ist. Sollten während der Migration Fehler auftreten, kann der Benutzer immer noch mit dem alten Computer arbeiten.

Wipe-and-Load-Migrationen

Für eine Migration auf denselben Computer ist es erforderlich, Benutzerdaten vom Computer an einem externen Ort zu speichern, beispielsweise auf einem USB-Speichergerät oder in einer Netzwerkfreigabe. Dann wird das vorhandene Betriebssystem gelöscht und eine Neuinstallation mit Windows 7 durchgeführt. Anschließend werden die Benutzerdaten vom externen Speicherort importiert. Nach dem erfolgreichen Abschluss der Migration können Sie die Benutzerdaten vom externen Speicherort löschen.

Migrationen auf denselben Computer sind dann sinnvoll, wenn Sie Windows 7 installieren müssen, aber keine direkte Aktualisierung durchführen können, weil auf dem Computer Windows XP oder eine Version von Windows Vista oder Windows 7 für eine andere Architektur installiert ist. Nehmen wir zum Beispiel an, Sie möchten das Betriebssystem auf einem Computer von Windows 7 Enterprise (x86) auf Windows 7 Enterprise (x64) umstellen. Der Nachteil einer Migration auf denselben Computer ist, dass der Benutzer nicht einfach mit der alten Konfiguration weiterarbeiten kann, falls die Migration fehlschlägt. Über die Migration von Daten erfahren Sie mehr in Lektion 3.

Übung Aktualisieren auf Windows 7

In dieser optionalen Übung aktualisieren Sie einen Windows Vista-Computer auf Windows 7. Sorgen Sie vor Beginn der Aktualisierung dafür, dass auf dem Windows Vista-Volume mindestens 10 GByte Speicherplatz frei sind. Die Übung lässt sich auch auf einem virtuellen Computer durchführen.

Übung 1 Aktualisieren von Windows Vista auf Windows 7

Überprüfen Sie vor Beginn der Aktualisierung, ob die Windows 7-Version für dieselbe Prozessorarchitektur ausgelegt ist wie die installierte Windows Vista-Version. Wenn Sie zum Beispiel eine x86-Version von Windows Vista aktualisieren möchten, brauchen Sie das Installationsmedium für die x86-Version von Windows 7. Gehen Sie folgendermaßen vor:

1. Melden Sie sich auf dem Windows Vista-Computer mit einem Konto an, das Mitglied der lokalen Gruppe *Administratoren* ist.
2. Legen Sie die DVD ein oder stellen Sie eine Verbindung mit der Windows 7-Installationsquelle her, falls Sie keine DVD verwenden, und klicken Sie *Setup.exe* doppelt an. Wenn sich die Benutzerkontensteuerung meldet, klicken Sie auf *Fortsetzen*. Dadurch wird der Windows-Installationsassistent geladen. Klicken Sie auf *Jetzt installieren*.
3. Klicken Sie auf der Seite *Laden Sie wichtige Updates für die Installation herunter* auf *Die neuesten Updates nicht für die Installation herunterladen*.
4. Überprüfen Sie auf der Seite *Lesen Sie bitte die Lizenzbedingungen* die Lizenzbedingungen für das Betriebssystem Windows 7 und wählen Sie das Kontrollkästchen *Ich akzeptiere die Lizenzbedingungen*, wenn Sie einverstanden sind. Klicken Sie auf *Weiter*.
5. Klicken Sie auf der Seite *Wählen Sie eine Installationsart aus* auf *Upgrade*. Der Installationsassistent überprüft die Kompatibilität und beginnt mit der Aktualisierung von Windows. Wie lange dieser Vorgang dauert, hängt von der Geschwindigkeit des Computers ab. Der Computer wird während des Vorgangs mehrmals neu gestartet.



Hinweis

Es ist möglich, die Aktualisierung nach einem Neustart des Computers durch die Wahl des Menüpunkts *Windows Setup-Zurücksetzung* aus dem Systemstartmenü rückgängig zu machen. Tun Sie das nur, wenn Sie die Aktualisierung tatsächlich rückgängig machen wollen oder noch einmal von vorne beginnen möchten.

6. Geben Sie auf der Seite *Geben Sie den Product Key ein* den Product Key für Windows 7 ein (Abbildung 1.16). Löschen Sie das Kontrollkästchen *Windows automatisch aktivieren, wenn eine Internetverbindung besteht* und klicken Sie auf *Weiter*.

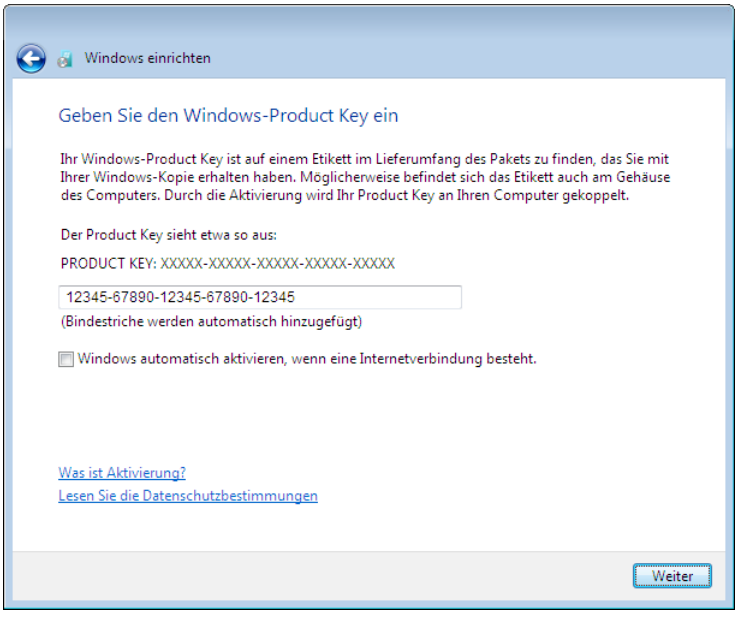

Windows einrichten
Geben Sie den Windows-Product Key ein
Ihr Windows-Product Key ist auf einem Etikett im Lieferumfang des Pakets zu finden, das Sie mit Ihrer Windows-Kopie erhalten haben. Möglicherweise befindet sich das Etikett auch am Gehäuse des Computers. Durch die Aktivierung wird Ihr Product Key an Ihren Computer gekoppelt.
Der Product Key sieht etwa so aus:
PRODUCT KEY: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
12345-67890-12345-67890-12345
(Bindestriche werden automatisch hinzugefügt)
Windows automatisch aktivieren, wenn eine Internetverbindung besteht.
Was ist Aktivierung?
Lesen Sie die Datenschutzbestimmungen
Weiter

Abbildung 1.16 Eingabe des Windows-Product Keys

7. Klicken Sie auf der Seite *Schützen Sie Ihren Computer, und verbessern Sie Windows automatisch* auf *Empfohlene Einstellungen verwenden*.
8. Überprüfen Sie auf der Seite *Überprüfen Sie die Zeit- und Datumseinstellungen* die Einstellung der Zeitzone und stellen Sie bei Bedarf Datum und Uhrzeit ein. Klicken Sie dann auf *Weiter*.
9. Klicken Sie auf der Seite *Wählen Sie den aktuellen Standort des Computers aus* auf *Heimnetzwerk*.
10. Melden Sie sich auf dem aktualisierten Computer mit den Anmeldeinformationen unter Windows 7 an, mit denen Sie sich zu Beginn dieser Übung unter Windows Vista angemeldet haben.
11. Fahren Sie den aktualisierten Windows 7-Computer herunter.

Zusammenfassung der Lektion

- Windows Vista lässt sich nur dann auf Windows 7 aktualisieren, wenn die Windows 7-Version für dieselbe Architektur vorgesehen ist (x86 oder x64) und einer gleichwertigen oder höheren Edition entspricht.
- Vor der Aktualisierung sollten Sie mit dem Windows 7 Upgrade Advisor überprüfen, ob sich die Hardware und die Software, die auf dem Windows Vista-Computer installiert ist, für Windows 7 eignen.
- Sie können eine Aktualisierung von einer Windows 7-Edition mit weniger Funktionen auf eine Edition mit mehr Funktionen durchführen, aber nicht von einer Edition mit mehr Funktionen auf eine mit weniger.
- Eine Aktualisierung von Windows XP auf Windows 7 ist nicht möglich.
- Side-by-Side-Migrationen sind Migrationen, bei denen Daten von einem Computer auf einen anderen übertragen werden, oder in Dual-Boot-Szenarien von einem Volume auf ein anderes.
- In Wipe-and-Load-Migrationen werden alle Benutzerdaten von einem Computer gesichert, die vorhandene Betriebssysteminstallation durch das neue Betriebssystem Windows 7 ersetzt und die Benutzerdaten wieder importiert.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 2, »Aktualisieren auf Windows 7«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Auf welche der folgenden Versionen und Editionen von Windows 7 können Sie einen Computer, auf dem Windows Vista Enterprise (x86) ausgeführt wird, direkt aktualisieren?
   A. Windows 7 Home Professional (x86).
   B. Windows 7 Ultimate (x86)
   C. Windows 7 Ultimate (x64)
   D. Windows 7 Enterprise (x64)
2. In welchen der folgenden Szenarien kommt nur eine Migration in Frage und keine Aktualisierung? (Wählen Sie alle zutreffenden Antworten.)
   A. Windows XP Professional (x64) auf Windows 7 Professional (x64)
   B. Windows Vista Business (x86) auf Windows 7 Professional (x64)
   C. Windows Vista Enterprise (x64) auf Windows 7 Enterprise (x64)
   D. Windows Vista Home Premium (x64) auf Windows 7 Home Premium (x86)

3. Ein Benutzer verfügt über einen Heimcomputer mit einer Internetverbindung. Weitere Computer stehen ihm nicht zur Verfügung. Mit welcher der folgenden Methoden kann der Benutzer eine Aktualisierung von Windows 7 Home Premium auf Windows 7 Ultimate durchführen?
   A. Sysprep
   B. Windows PE
   C. WDS
   D. Windows Anytime Upgrade
4. Mit welchem der folgenden Tools können Sie überprüfen, ob Anwendungen, die Sie auf einem Windows Vista-Computer installiert haben, unter Windows 7 Kompatibilitätsprobleme aufweisen?
   A. Windows 7 Upgrade Advisor
   B. Sysprep
   C. USMT
   D. Windows PE
5. Auf welche der folgenden Editionen und Versionen von Windows 7 können Sie einen Computer aktualisieren, auf dem Windows 7 Home Premium (x86) ausgeführt wird? (Wählen Sie alle zutreffenden Antworten.)
   A. Windows 7 Professional (x86)
   B. Windows 7 Professional (x64)
   C. Windows 7 Ultimate (x86)
   D. Windows 7 Enterprise (x64)

Lektion 3: Verwalten von Benutzerprofilen

Sofern Sie keine direkte Aktualisierung von Windows Vista auf Windows 7 durchführen oder einen Computer aktualisieren, der mit servergespeicherten Benutzerprofilen arbeitet, ist es für jede Windows 7-Bereitstellung erforderlich, einen Plan für die Übertragung der Benutzerprofildaten vom alten auf den neuen Computer zu entwickeln. Die Übernahme der vorhandenen Benutzerdaten wie E-Mails oder Webbrowser-Lesezeichen ist bei der Durchführung einer Windows 7-Bereitstellung ebenso wichtig wie die Auswahl der richtigen Hardwareplattform. Wenn Sie nicht alle Daten der Benutzer von den alten auf die neuen Computer übertragen, können die Benutzer vielleicht nicht mehr ihre Arbeit erledigen. Außerdem können sich Benutzer in einem neuen Betriebssystem schneller orientieren, wenn sie ihre gewohnten Einstellungen bereits bei der ersten Anmeldung auf dem neuen System vorfinden. Je einfacher der Umstieg für die Benutzer wird, desto positiver beurteilen sie den Wechsel. In dieser Lektion erfahren Sie, wie Sie Benutzerdaten von einer alten Windows-Installation oder von einer vorhandenen Windows 7-Installation auf eine neue Windows 7-Installation übertragen können.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Migrieren der Benutzerprofile von einem Windows 7-Computer auf einen anderen
- Migrieren der Benutzerprofile von einer älteren Windows-Version

Veranschlagte Zeit für diese Lektion: 40 Minuten

Migrieren von Benutzerprofildaten

Benutzerdaten bestehen aus mehr als nur den Dokumenten, die in einem Textverarbeitungsprogramm erstellt wurden. Zu den Benutzerdaten gehören zum Beispiel die Favoritenliste des Internetbrowsers, angepasste Anwendungsdaten wie beispielsweise E-Mail-Kontendaten, Desktophintergründe, Dateien und Ordner. Wenn Sie in Ihrer Organisation keine servergespeicherten Benutzerprofile verwenden, sind auf den Computern der Benutzer wahrscheinlich wichtige Daten gespeichert. Zur erfolgreichen Migration eines Benutzers von Windows XP oder Windows Vista nach Windows 7 müssen Sie sicherstellen, dass alle wichtigen Benutzerdaten vom alten auf den neuen Computer übernommen werden.

Wenn Sie überprüfen möchten, welche Benutzerprofile auf einem Windows 7-Computer gespeichert sind, öffnen Sie die Systemsteuerung, klicken auf *System und Sicherheit*, dann auf *System* und schließlich auf *Erweiterte Systemeinstellungen*. Klicken Sie dann auf der Registerkarte *Erweitert* des Dialogfelds *Systemeigenschaften* im Abschnitt *Benutzerprofile* auf die Schaltfläche *Einstellungen*. Es öffnet sich das Dialogfeld *Benutzerprofile* (Abbildung 1.17), in dem Sie die Größe der Benutzerprofile überprüfen und Benutzerprofile löschen oder von lokalen in servergespeicherte Benutzerprofile konvertieren können.

Ein servergespeichertes Benutzerprofil ist ein Profil, das auf einem Server gespeichert und auf jedem Windows 7-Computer eines Netzwerks verfügbar ist. Administratoren implementieren servergespeicherte Benutzerprofile, wenn die Benutzer nicht immer an demselben Computer arbeiten, sondern sich praktisch an jedem Computer der Organisation anmelden können sollen. Servergespeicherte Benutzerprofile ermöglichen zudem eine zentrale Sicherung der Benutzerdaten.

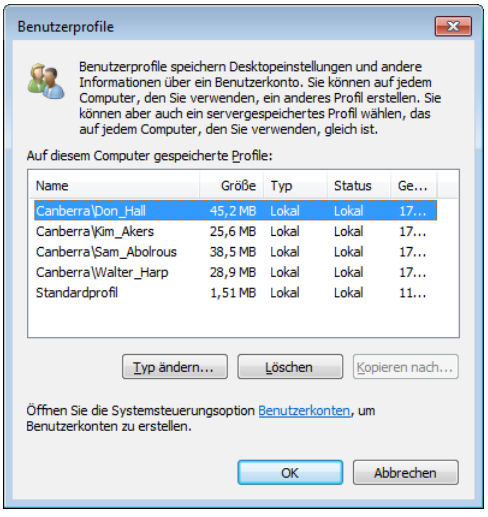

Benutzerprofile
Benutzerprofile speichern Desktopeinstellungen und andere Informationen über ein Benutzerkonto. Sie können auf jedem Computer, den Sie verwenden, ein anderes Profil erstellen. Sie können aber auch ein servergespeichertes Profil wählen, das auf jedem Computer, den Sie verwenden, gleich ist.
Auf diesem Computer gespeicherte Profile:
Name Größe Typ Status Ge...
Canberra\Don_Hall 45,2 MB Lokal Lokal 17...
Canberra\Kim_Akers 25,6 MB Lokal Lokal 17...
Canberra\Sam_Abolrous 38,5 MB Lokal Lokal 17...
Canberra\Walter_Harp 28,9 MB Lokal Lokal 17...
Standardprofil 1,51 MB Lokal Lokal 11...
Typ ändern... Löschen Kopieren nach...
Öffnen Sie die Systemsteuerungsoption Benutzerkonten, um Benutzerkonten zu erstellen.
OK Abbrechen

Abbildung 1.17 Eine Liste der Benutzerprofile

Windows-EasyTransfer

Windows-EasyTransfer ist ein Hilfsprogramm von Windows 7, mit dem Sie Benutzerprofildaten von Computern, auf denen Windows XP, Windows Vista oder Windows 7 ausgeführt wird, auf neue Windows 7-Computer übertragen können. Wie aus Abbildung 1.18 hervorgeht, eignet sich Windows-EasyTransfer für die Übertragung von Benutzerkonten, Dokumenten, Musik, Bildern, E-Mails, Zertifikaten und anderer Daten.


Windows-EasyTransfer
Willkommen
Mithilfe von Windows-EasyTransfer können Dateien und Einstellungen eines Computers an einen anderen Computer übertragen werden. Vom Quellcomputer werden keine Informationen gelöscht.
Sie können Folgendes übertragen:
Benutzerkonten
Dokumente
Musik
Bilder
E-Mail
Internetfavoriten
Videos
Und mehr
Nach dem Abschluss der Übertragung wird eine Liste der übertragenen Elemente angezeigt. Zudem werden Programme, die Sie möglicherweise auf dem Zielcomputer installieren möchten, sowie Links zu anderen Programmen, die Sie möglicherweise herunterladen möchten, angezeigt.
Tipp: Falls Sie ein Upgrade auf Windows 7 durchführen, stellen Sie sich den Quellcomputer als Ihre alte Windows-Version und den Zielcomputer als die neue Windows-Version vor.
Weiter

Abbildung 1.18 Die Willkommensseite von Windows-EasyTransfer

Es gibt drei verschiedene Methoden, Daten mit Windows-EasyTransfer zu migrieren. Welche Methode sich am besten eignet, hängt von der jeweiligen Situation ab. Zur Migration von Profildaten mit Windows-EasyTransfer können Sie Folgendes verwenden:

- **EasyTransfer-Kabel** Das ist ein spezielles Kabel mit USB-Steckern, das von Hardwareherstellern angeboten wird. Das eine Ende verbinden Sie mit dem Quellcomputer, das andere mit dem Zielcomputer. Beide Computer werden für die Migration eingeschaltet und auf beiden Computern wird Windows-EasyTransfer ausgeführt. Mit dieser Methode können Sie nur Migrationen auf andere Computer (Side-by-Side) durchführen.
- **Netzwerk** Um die Migration über das Netzwerk durchzuführen, müssen der Quell- und der Zielcomputer am selben lokalen Netzwerk angeschlossen sein. Während der Migration müssen beide Computer eingeschaltet sein und auf beiden muss Windows-EasyTransfer ausgeführt werden. Mit dieser Methode können Sie nur eine Migration auf einen anderen Computer durchführen. Wenn Sie eine Migration über ein Netzwerk durchführen, legen Sie auf dem Quellcomputer ein Kennwort fest. Dieses Kennwort müssen Sie auch auf dem Zielcomputer eingeben.
- **Externe Festplatte oder USB-Flashlaufwerk** Als Speichermedium für die Benutzerdaten können Sie auch eine angeschlossene externe Festplatte oder ein USB-Flashlaufwerk verwenden. Es ist bei dieser Methode auch möglich, ein internes Festplattenlaufwerk oder eine Netzwerkfreigabe zu verwenden. Sie können Migrationen von einem Computer auf einen anderen durchführen oder auf demselben Computer. Die Daten schützen Sie auf dem Quellcomputer mit einem Kennwort, das Sie auf dem Zielcomputer wieder eingeben müssen, um die Daten importieren zu können.

Installieren von Windows-EasyTransfer

Sofern auf dem Quellcomputer nicht Windows 7 verwendet wird, müssen Sie die Windows-EasyTransfer-Anwendung installieren. Das gilt auch für Quellcomputer, auf denen Windows Vista verwendet wird. In Windows Vista gibt es zwar eine ältere Version der Windows-EasyTransfer-Software, aber Sie sollten für die Datenübertragung auf Windows 7-Computer die aktuellere Windows 7-Version verwenden. Die Installation von Windows-EasyTransfer auf dem Quellcomputer ist nicht schwer:

1. Starten Sie auf dem Zielcomputer Windows-EasyTransfer und wählen Sie die Übertragungsmethode aus, die Sie verwenden möchten.
2. Wählen Sie die Option *Dies ist der Zielcomputer*. Wenn Sie das EasyTransfer-Kabel oder das Netzwerk gewählt haben, fahren Sie mit Schritt 3 fort. Andernfalls klicken Sie auf *Nein*, wenn Sie gefragt werden, ob Windows-EasyTransfer Ihre Daten bereits gespeichert hat.
3. Wählen Sie auf der Seite *Müssen Sie Windows-EasyTransfer auf dem Quellcomputer installieren?* die Option *Ich muss das Programm jetzt installieren* (Abbildung 1.19).
4. Wählen Sie auf der Seite *Wie soll Windows-EasyTransfer auf dem Quellcomputer installiert werden?* entweder das USB-Flashlaufwerk oder die externe Festplatte oder den freigegebenen Netzwerkordner aus. Die Installationsdatei der Windows-EasyTransfer-Anwendung wird an den angegebenen Ort kopiert. Anschließend können Sie die Anwendung auf dem Quellcomputer installieren.

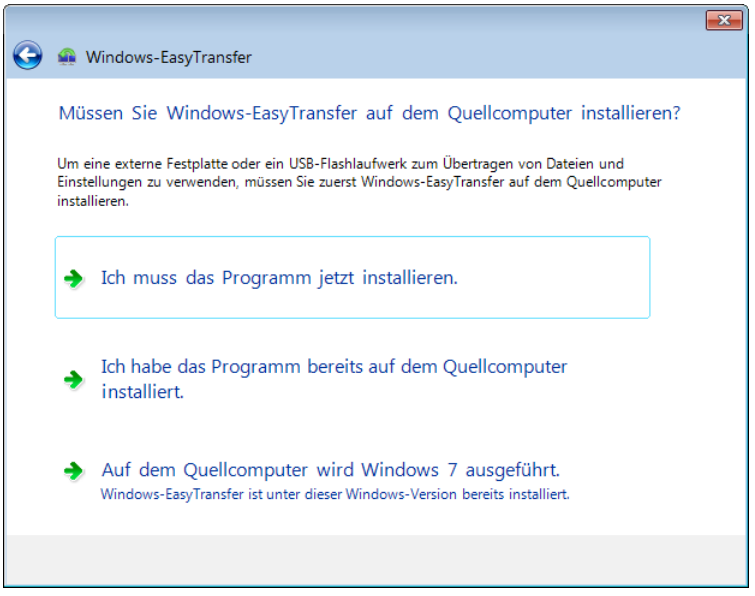

Windows-EasyTransfer
Müssen Sie Windows-EasyTransfer auf dem Quellcomputer installieren?
Um eine externe Festplatte oder ein USB-Flashlaufwerk zum Übertragen von Dateien und Einstellungen zu verwenden, müssen Sie zuerst Windows-EasyTransfer auf dem Quellcomputer installieren.
Ich muss das Programm jetzt installieren.
Ich habe das Programm bereits auf dem Quellcomputer installiert.
Auf dem Quellcomputer wird Windows 7 ausgeführt.
Windows-EasyTransfer ist unter dieser Windows-Version bereits installiert.

Abbildung 1.19 Bereiten Sie die Windows-EasyTransfer-Installationsdateien vor

Migrieren mit Windows-EasyTransfer

Nachdem Sie Windows-EasyTransfer auf dem Quellcomputer eingerichtet haben, kann die Migration beginnen. Wenn Sie nur ein einzelnes Benutzerkonto migrieren möchten, können Sie sich mit diesem Konto anmelden, um die Übertragung durchzuführen. Wollen Sie alle Konten migrieren, die sich auf dem Computer befinden, müssen Sie sich mit einem Konto anmelden, das über die Rechte eines lokalen Administrators verfügt. Dann starten Sie Windows-EasyTransfer, wählen die Übertragungsmethode und klicken auf der Seite *Welchen Computer verwenden Sie jetzt?* auf *Dies ist der Quellcomputer*. Wenn Sie eine externe Festplatte oder ein USB-Speichergerät verwenden, überprüft Windows-EasyTransfer dann den Platzbedarf der Daten, die auf den neuen Computer übertragen werden. Wenn Sie die Daten über das Netzwerk oder über ein EasyTransfer-Kabel übertragen, wählen Sie nun die Elemente aus, die auf den Zielcomputer übertragen werden sollen.

Sie können die Standardauswahl der zu migrierenden Elemente übernehmen oder die Auswahl für jedes Benutzerkonto und die öffentlichen Elemente ändern. Dazu klicken Sie unter den einzelnen Konten auf *Anpassen*. Anschließend können Sie jeweils festlegen, ob die Bilder, Dokumente, Musik, Videos und Windows-Einstellungen des Benutzerprofils übertragen werden sollen. Wenn Sie die Auswahl noch genauer treffen möchten, können Sie auf *Erweitert* klicken, um das Dialogfeld *Auswahl ändern* zu öffnen (Abbildung 1.20). In diesem Dialogfeld können Sie festlegen, welche Benutzerprofile migriert werden sollen und welche Dateien und Ordner Windows-EasyTransfer auf den neuen Computer überträgt.

Die ersten Schritte bei der Verwendung von Windows-EasyTransfer auf dem Zielcomputer sind die Angaben der Übertragungsmethode und des Zielcomputers. Je nach der verwendeten Methode geschieht Folgendes:

- Wenn Sie eine externe Festplatte oder ein USB-Flashlaufwerk verwenden, werden Sie aufgefordert, den Speicherort der EasyTransfer-Datei und das Kennwort einzugeben, um die Datei zu öffnen.

- Wenn Sie ein Netzwerk verwenden, müssen Sie den Windows-EasyTransfer-Schlüssel eingeben, bevor die Übertragung beginnt. Dieser Schlüssel wird auf dem Quellcomputer angezeigt. Anschließend legen Sie wie bereits beschrieben fest, was übertragen werden soll.
- Wenn Sie ein EasyTransfer-Kabel verwenden, versucht der Assistent, das Kabel zu erkennen und die Übertragung zu starten. Anschließend wählen Sie wie bereits beschrieben aus, was übertragen werden soll.

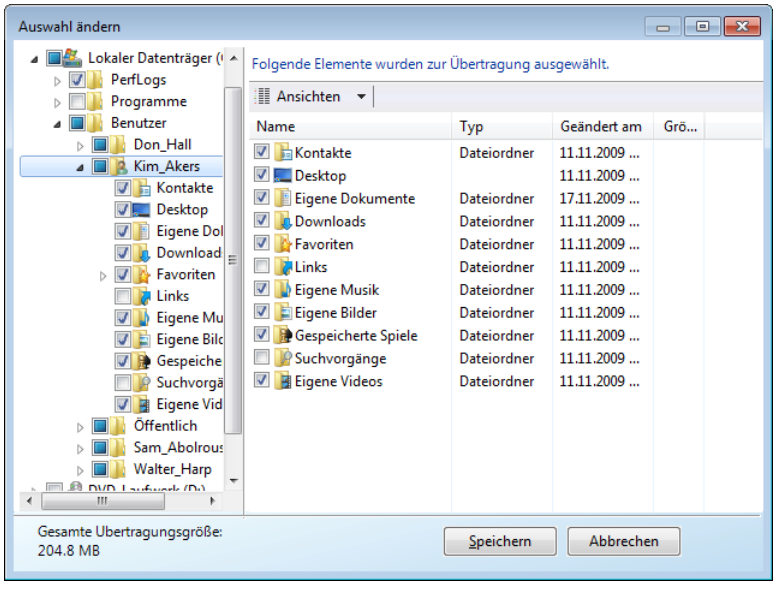


Abbildung 1.20 Auswahl der Daten, die von Windows-EasyTransfer übertragen werden

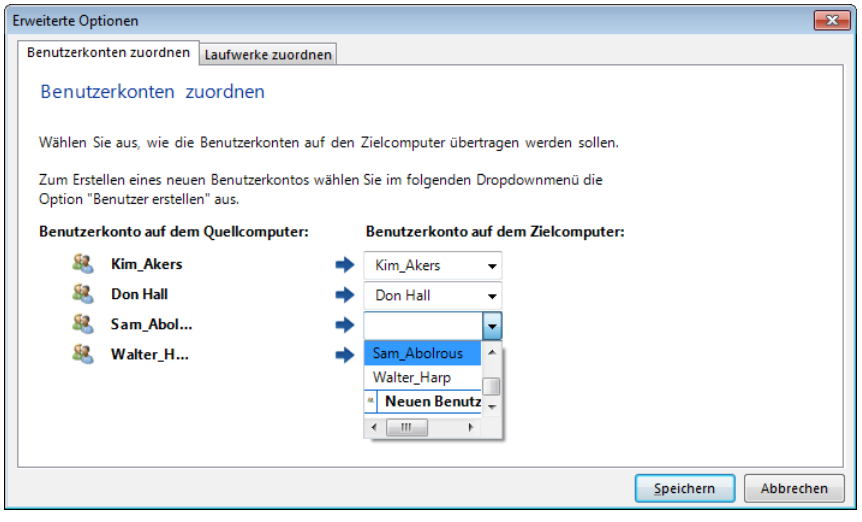


Abbildung 1.21 Kontenübertragung mit Windows-EasyTransfer

Wenn Sie *Erweiterte Optionen* wählen, können Sie genauer festlegen, was mit den Benutzerkonten geschehen soll, die vom Quellcomputer auf den Zielcomputer übertragen werden. Sie können ein Benutzerkonto vom alten Computer zum Beispiel auf ein bestimmtes Benutzerkonto des neuen Computers abbilden oder Windows-EasyTransfer ein neues Konto anlegen lassen (Abbildung 1.21). Wenn Sie die Option *Neuen Benutzer erstellen* wählen, müssen Sie einen Namen und ein Kennwort für das neue Konto festlegen. Wenn Sie *Erweiterte Optionen* nicht wählen, erstellt Windows-EasyTransfer auf dem Windows 7-Computer Konten mit den alten Namen, aber ohne Kennwörter. Bei der ersten Anmeldung müssen die Benutzer ihre Kennwörter festlegen.

In der Übung am Ende der Lektion führen Sie eine Migration mit Windows-EasyTransfer durch.

Schnelltest

- Welche Windows-EasyTransfer-Übertragungsmethode sollten Sie bei einer Migration auf denselben Computer (Wipe-and-Load) verwenden?

Antwort zum Schnelltest

- Die einzige Windows-EasyTransfer-Übertragungsmethode, die sich für Migrationen auf denselben Computer eignet, ist die Methode externe Festplatte oder USB-Flashlaufwerk.

User State Migration Tool

USMT 4.0 ist ein Befehlszeilenprogramm, mit dem Sie die Benutzerprofilmigration automatisieren können. USMT ist Teil des Windows Automated Installation Kit (WAIK) und eignet sich für die Übertragung einer großen Zahl von Benutzerprofilen besser als Windows-EasyTransfer. USMT kann Daten auf USB-Wechseldatenträger oder auf eine Netzwerkfreigabe schreiben, aber keine direkten Migrationen vom Quellcomputer über das Netzwerk auf den Zielcomputer durchführen. Es unterstützt auch keine Migrationen mit dem Windows-EasyTransfer-Kabel. USMT-Migrationen erfolgen in zwei Phasen: Zuerst werden die Profile auf dem Quellcomputer mit ScanState exportiert und dann auf dem Zielcomputer mit LoadState importiert.

USMT 4.0 ermöglicht Ihnen die Übertragung von Benutzerkonten, Benutzerdateien sowie Betriebssystem- und Anwendungseinstellungen. Außerdem überträgt USMT Zugangssteuerungslisten (Access Control Lists, ACLs) für Dateien und Ordner und sorgt auf diese Weise dafür, dass die auf dem Quellcomputer eingestellten Berechtigungen auf den Zielcomputer übernommen werden. Sie können mit USMT Profildaten von Computern erfassen, auf denen Windows XP, Windows Vista oder Windows 7 verwendet wird, und auf Windows 7-Computer übertragen. Außerdem können Sie mit USMT Daten von Windows 7-Computern auf Windows Vista-Computer übertragen. Mit USMT können Sie keine zugeordneten Netzwerklaufwerke migrieren, keine lokalen Drucker, Gerätetreiber, Kennwörter, Berechtigungen für freigegebene Ordner und keine Einstellungen für gemeinsam verwendete Internetverbindungen.



Hinweis USMT und Downgrades

Sie können USMT nicht verwenden, um Daten von Windows 7-Computern auf Computer zu übertragen, auf denen Windows XP verwendet wird.

Anders als bei Windows-EasyTransfer, wo Sie die zu übertragenden Elemente in der Anwendung auswählen können, konfigurieren Sie für USMT vor der Übertragung Migrationsregeln, mit denen festgelegt wird, welche Daten vom Quellcomputer exportiert werden.

USMT verwendet vier verschiedene *.xml*-Migrationsdateien:

- ***MigApp.xml*** Diese Datei enthält Regeln für die Übertragung von Anwendungseinstellungen. Dazu gehören Barrierefreiheitseinstellungen, Einwählverbindungen, Favoriten, Ordnereinstellungen, Gruppenmitgliedschaften, ODBC-Einstellungen (Open Database Connectivity), Postfachdateien für Microsoft Office Outlook Express, Maus- und Tastatureinstellungen, Telefon- und Modemeinstellungen, RAS-Telefonbücher (Remote Access Service), Regionseinstellungen und Einstellungen für Remotezugriff, Bildschirmschoner, Taskleiste und Bildschirmhintergrund.



Weitere Informationen Migrieren von benutzerdefinierten Anwendungen

Mit *MigApp.xml* können Sie bei einigen benutzerdefinierten Anwendungen die Einstellungen nicht übernehmen. In diesem Fall müssen Sie eine spezielle XML-Datei (Extensible Markup Language) erstellen. Im Microsoft TechNet finden Sie unter *http://technet.microsoft.com/en-us/library/dd560773(WS.10).aspx* eine Beschreibung, wie man diese benutzerdefinierte XML-Datei erstellt.

- ***MigUser.xml*** Diese Datei enthält Regeln für Benutzerprofile und Benutzerdaten. Mit den Standardeinstellungen werden alle Daten aus den Ordnern *Eigene Dokumente*, *Eigene Videos*, *Eigene Musik*, *Eigene Bilder*, *Desktop*, *Startmenü*, *Quick Launch*, *Favoriten*, *Gemeinsame Dokumente*, *Gemeinsame Videos*, *Gemeinsame Musik*, gemeinsame Desktopdateien, *Gemeinsame Bilder*, gemeinsame Startmenüeinträge und gemeinsame Favoriten übertragen. Außerdem enthält die Datei Regeln für die Übertragung folgender Dateitypen von fest installierten Volumes: *.qdf*, *.qsd*, *.qel*, *.qph*, *.doc*, *.dot*, *.rtf*, *.mcw*, *.wps*, *.scd*, *.wri*, *.wpd*, *.xl**, *.csv*, *.iqy*, *.dqy*, *.oqy*, *.rqy*, *.wk**, *.wq1*, *.slk*, *.dif*, *.ppt**, *.pps**, *.pot**, *.sh3*, *.ch3*, *.pre*, *.ppa*, *.txt*, *.pst*, *.one**, *.mpp*, *.vsd*, *.vl**, *.or6*, *.accdb*, *.mdb*, *.pub*, *.xla*, *.xlb* und *.xls*. Das Sternchen (*) steht für null oder mehr Zeichen.
- ***MigDocs.xml*** Diese Datei enthält Informationen über die Speicherorte der Benutzerdokumente.
- ***Config.xml*** Diese Datei unterscheidet sich von den anderen Migrationsdateien, da sie dazu verwendet wird, Dateien von der Übertragung auszuschließen. Sie können die Datei *Config.xml* erstellen und ändern, indem Sie *ScanState.exe* mit der Option `/genconfig` verwenden.

Bei der Übertragung lassen sich auch benutzerdefinierte XML-Dateien verwenden. Sie können zum Beispiel eine XML-Datei erstellen, die Ordner, bestimmte Dateitypen oder bestimmte Dateien umleitet. Eine Umleitung kann sinnvoll sein, um alle Dateien eines bestimmten Typs, beispielsweise *.avi*-Dateien, die auf dem Quellcomputer an verschiedenen

Orten gespeichert sind, auf dem Zielcomputer in einem bestimmten Ordner zusammenzufassen.



Weitere Informationen Umleiten von Dateien und Einstellungen

Weitere Informationen über die Umleitung von Dateien und Einstellungen mit USMT finden Sie auf der folgenden Webseite im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/dd560798.aspx*.

ScanState

Während der Migration verwenden Sie ScanState auf dem Quellcomputer. Unter Windows Vista und Windows 7 müssen Sie *ScanState.exe* in einer Eingabeaufforderung mit erhöhten Rechten verwenden. Auf einem Windows XP-Quellcomputer müssen Sie sich als ein Benutzer anmelden, der Mitglied der lokalen Gruppe *Administratoren* ist, um ScanState verwenden zu können.

Der folgende Befehl erstellt auf der Dateifreigabe *Migration* eines Servers namens *Dateiserver* einen verschlüsselten Speicher namens *MeinSpeicher*, wobei der Schlüssel *MeinSchluessel* verwendet wird:

```
scanstate \\Dateiserver\Migration\MeinSpeicher /i:MigApp.xml /i:MigUser.xml /o
/config:Config.xml /encrypt /key:"MeinSchluessel"
```

Wenn Sie ScanState und LoadState mit der Option `/v:13` verwenden, wird eine ausführliche Protokolldatei erstellt. Verwenden Sie diese Option, wenn sich bei der Migration der Daten Probleme ergeben.



Weitere Informationen ScanState

Weitere Informationen über die ScanState-Syntax finden Sie auf der folgenden Webseite im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/dd560781.aspx*.

LoadState

LoadState wird auf dem Zielcomputer ausgeführt. Sie sollten alle Anwendungen, die auf dem Quellcomputer installiert sind, auch auf dem Zielcomputer installieren, bevor Sie LoadState verwenden. Unter Windows 7 und Windows Vista müssen Sie *LoadState.exe* in einer Eingabeaufforderung mit erhöhten Rechten ausführen.

Um die Profildaten aus einem verschlüsselten Speicher namens *MeinSpeicher* zu laden, der auf einem Dateiserver namens *Dateiserver* in der Freigabe *Migration* gespeichert und mit dem Verschlüsselungsschlüssel *MeinSchluessel* verschlüsselt wurde, verwenden Sie folgenden Befehl:

```
loadstate \\Dateiserver\Migration\MeinSpeicher /i:MigApp.xml /i:MigUser.xml /decrypt
/key:"MeinSchluessel"
```



Weitere Informationen LoadState

Weitere Informationen über die LoadState-Syntax finden Sie auf folgender Webseite im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/dd560804.aspx*.

Migrationsspeichertypen

Bei der Planung einer Migration mit USMT müssen Sie festlegen, wo die migrierten Daten gespeichert werden sollen, die ScanState auf dem Quellcomputer erfasst und die LoadState für die Übernahme der Daten auf den Zielcomputer braucht. USMT unterstützt drei Arten von Migrationsspeichern:

- **Unkomprimiert** Ein unkomprimierter Migrationsspeicher speichert eine Ordnerhierarchie, die das zu übertragende Benutzerprofil nachbildet. Es wird praktisch eine Kopie des Benutzerprofils erstellt. Sie können mit dem Windows-Explorer im unkomprimierten Migrationsspeicher navigieren.
- **Komprimiert** Ein komprimierter Migrationsspeicher besteht aus einer einzigen Abbilddatei, die alle zu übertragenden Daten enthält. Die Abbilddatei kann verschlüsselt und mit einem Kennwort geschützt werden. Es ist nicht möglich, mit dem Windows-Explorer in dieser Datei zu navigieren.
- **Hard-link** Hard-link-Migrationsspeicher werden nur bei Migrationen auf denselben Computer (Wipe-and-Load) verwendet. Der Hard-link-Migrationsspeicher wird auf dem lokalen Computer erstellt. Anschließend wird das alte Betriebssystem entfernt und das neue installiert. Um einen Hard-link-Migrationspeicher zu erstellen, verwenden Sie ScanState mit der Option `/hardlink`. Bei dieser »festen Zuordnung« werden keine Duplikate der zu übertragenden Daten erstellt. Der zusätzliche Platzbedarf ist also geringer als bei der Übertragung der Daten mit einem komprimierten oder unkomprimierten Speicher. Für eine Hard-link-Migration ist auf dem Volume, auf dem die zu übertragenden Daten liegen, unabhängig von deren Menge nur ungefähr 250 MByte freier Speicherplatz erforderlich.

ScanState mit der Option `/p` ermöglicht vor der Durchführung der Migration eine Abschätzung der Größe des Migrationsspeichers. Für jede Migration ist auf dem Volume, auf dem die zu übertragenden Daten liegen, mindestens 250 MByte freier Speicherplatz erforderlich.



Weitere Informationen Migrationsspeichertypen

Weitere Informationen über USMT-Migrationsspeichertypen erhalten Sie in dem folgendem Artikel im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/dd560795.aspx*.

Durchführen von Offline-Migrationen

Sie können auch Offline-Migrationen mit USMT durchführen. Bei Offline-Migrationen wird der Quellcomputer in eine Windows PE-Umgebung gestartet, in der die USMT-Dateien zur Verfügung stehen. Dann werden die gewünschten Daten mit ScanState von der Windows-Installation auf der Festplatte des Computers gelesen. LoadState lässt sich aber nicht in einer Windows PE-Umgebung ausführen, sondern muss auf dem Zielcomputer unter Windows 7 verwendet werden.



Hinweis ScanState und Upgrades

Sie können auch das Verzeichnis *Windows.old*, das bei der Durchführung einer Aktualisierung von Windows Vista angelegt wird, offline mit ScanState bearbeiten.

Offline-Migrationen haben den Vorteil, dass auf den Quellcomputer kein Zugriff mit Administratorrechten erforderlich ist. Einen Computer, der mit BitLocker geschützt ist, können Sie nicht offline migrieren. Damit USMT Zugriff auf alle zu übertragenden Dateien erhält, ist es erforderlich, BitLocker für den betreffenden Zeitraum anzuhalten (suspend).



Weitere Informationen Offline-Migrationen

Weitere Informationen über Offline-Migrationen mit USMT finden Sie auf der folgenden Seite im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/dd560758.aspx*.

Übung Migrieren von Benutzerdaten

Wenn beim Wechsel auf die gewünschte Windows 7-Edition keine direkte Aktualisierung möglich ist, bietet sich eine Migration an. Außerdem kann eine Migration notwendig sein, wenn Sie Benutzerdaten von einem Windows 7-Computer auf einen anderen übertragen müssen. Es gibt zwei Tools, mit denen Sie Benutzerprofildaten zuverlässig von einem Computer auf einen anderen übertragen können: USMT und Windows-EasyTransfer.

Übung 1 Migrieren von Benutzerdaten mit Windows-EasyTransfer

In dieser Übung erstellen Sie ein Benutzerkonto und Benutzerdaten, übertragen diese Daten mit Windows-EasyTransfer auf ein USB-Gerät, entfernen die Benutzerdaten vom Computer und migrieren das Benutzerkonto mit Windows-EasyTransfer zurück auf den Computer, um die Migration des Benutzers auf einen anderen Windows 7-Computer zu simulieren.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers*, das Sie in der Übung von Lektion 1 erstellt haben, beim Computer *Canberra* an.
2. Klicken Sie auf *Start* und *Systemsteuerung*. Klicken Sie unter *Benutzerkonten und Jugendschutz* auf *Benutzerkonten hinzufügen/entfernen*.
3. Klicken Sie auf der Seite *Konten verwalten* auf *Neues Konto erstellen*. Geben Sie als Kontonamen **Don_Hall** ein und machen Sie das Konto zu einem *Standardbenutzer*.
4. Klicken Sie das Konto *Don_Hall* auf der Seite *Konten verwalten* an und klicken Sie dann auf *Kennwort erstellen*. Geben Sie zweimal das Kennwort **P@ssw0rd** ein. Im Textfeld *Kennworthinweis* geben Sie die Seitennummer dieses Buchs ein. Klicken Sie auf *Kennwort erstellen* und schließen Sie dann die Systemsteuerung.
5. Klicken Sie auf *Start*. Klicken Sie auf den Pfeil neben *Herunterfahren* und dann auf *Benutzer wechseln*. Melden Sie sich mit dem Benutzerkonto *Don_Hall* an.
6. Wenn Sie mit dem Benutzerkonto *Don_Hall* auf dem Computer *Canberra* angemeldet sind, klicken Sie den Desktop mit der rechten Maustaste an und klicken dann auf *Neu*, *Textdokument*. Nennen Sie das Textdokument **Migrationstest.txt.** Öffnen Sie die Datei und geben Sie **Migrationstest** ein. Speichern Sie das Dokument und schließen Sie den Editor.
7. Melden Sie sich mit dem Benutzerkonto *Don_Hall* ab und dann wieder mit dem Benutzerkonto *Kim_Akers* an.
8. Schließen Sie das USB-Speichergerät an, auf dem Sie die Benutzerprofildaten speichern möchten.
9. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Windows-EasyTransfer** ein und drücken Sie die EINGABETASTE.

10. Klicken Sie auf der Willkommensseite auf *Weiter*. Klicken Sie auf der Seite *Was möchten Sie verwenden, um Elemente auf den Zielcomputer zu übertragen?* auf *Eine externe Festplatte oder ein USB-Flashlaufwerk*.
11. Klicken Sie auf der Seite *Welchen Computer verwenden Sie jetzt?* auf *Dies ist der Quellcomputer*.
12. Windows-EasyTransfer überprüft dann, welche Informationen übertragen werden können. Sorgen Sie auf der Seite *Wählen Sie aus, was von diesem Computer übertragen werden soll* dafür, dass nur das Benutzerkonto *Don_Hall* gewählt ist (Abbildung 1.22). Das Konto *Kim_Akers* oder die freigegebenen Elemente brauchen Sie in dieser Übung nicht zu migrieren. Klicken Sie auf *Weiter*.

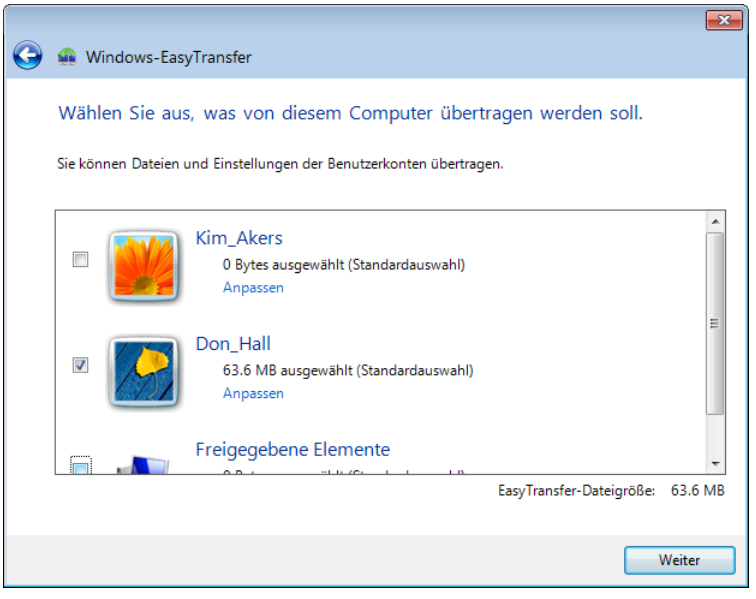


Abbildung 1.22 Wählen Sie die zu migrierenden Elemente aus

13. Geben Sie auf der Seite *Speichern Sie die zu übertragenden Dateien und Einstellungen* zweimal das Kennwort **P@ssw0rd** ein und klicken Sie dann auf *Speichern*.
14. Geben Sie im Dialogfeld *Speichern der EasyTransfer-Datei* das USB-Speichergerät an, das Sie in Schritt 8 an den Computer angeschlossen haben, und klicken Sie dann auf *Speichern*. Nach dem Abschluss der Speicherung der Daten auf dem USB-Speichergerät klicken Sie zweimal auf *Weiter* und dann auf *Schließen*.
15. Klicken Sie auf *Start*, dann mit der rechten Maustaste auf *Computer* und wählen Sie *Eigenschaften*. Klicken Sie auf *Erweiterte Systemeinstellungen*. Im Dialogfeld *Systemeigenschaften* klicken Sie im Bereich *Benutzerprofile* auf die Schaltfläche *Einstellungen*, um das Dialogfeld *Benutzerprofile* zu öffnen (Abbildung 1.23).
16. Wählen Sie das Profil *Canberra\Don_Hall* aus und klicken Sie dann auf *Löschen*. Wenn Sie aufgefordert werden, die Löschung zu bestätigen, klicken Sie auf *Ja*. Klicken Sie zweimal auf *OK*, um die Dialogfelder *Benutzerprofile* und *Systemeigenschaften* zu schließen.

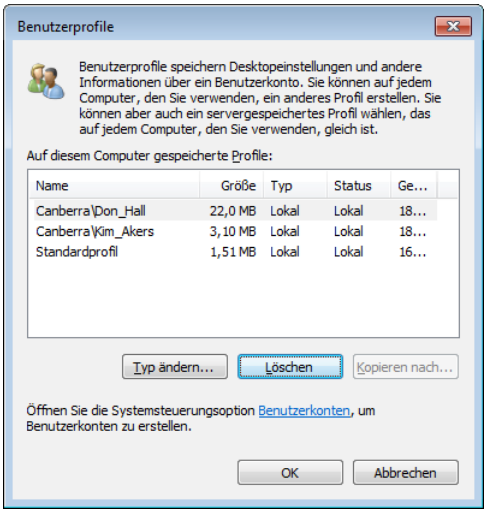


Abbildung 1.23 Die Benutzerprofilliste

17. Klicken Sie auf *Start* und dann auf *Systemsteuerung*. Klicken Sie unter *Benutzerkonten und Jugendschutz* auf *Benutzerkonten hinzufügen/entfernen*.
18. Wählen Sie das Konto *Don_Hall* aus und klicken Sie dann auf *Konto löschen*. Klicken Sie auf der Seite *Möchten Sie die Dateien von Don_Hall behalten?* auf *Dateien löschen*. Klicken Sie auf *Konto löschen* und schließen Sie die Systemsteuerung.
19. Melden Sie sich ab und überprüfen Sie, ob es noch möglich ist, sich mit dem Konto *Don_Hall* am Computer *Canberra* anzumelden.
20. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* an.
21. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Windows-EasyTransfer** ein und drücken Sie dann die EINGABETASTE. Klicken Sie auf der Willkommensseite auf *Weiter*.
22. Klicken Sie auf der Seite *Was möchten Sie verwenden, um Elemente auf den Zielcomputer zu übertragen?* auf *Eine externe Festplatte oder ein USB-Flashlaufwerk*.
23. Klicken Sie auf der Seite *Welchen Computer verwenden Sie jetzt?* auf *Dies ist der Zielcomputer*.
24. Klicken Sie auf der Seite *Wurden Ihre Dateien bereits vom Quellcomputer auf einer externen Festplatte oder einem USB-Flashlaufwerk gespeichert?* auf *Ja*.
25. Navigieren Sie zu dem Ort auf dem USB-Speichergerät, an dem Sie die Migrationsdaten in Schritt 14 gespeichert haben. Wählen Sie die Datei *Windows-EasyTransfer – Elemente vom Quellcomputer* aus und klicken Sie auf *Öffnen*. Geben Sie das Kennwort **P@ssw0rd** ein**.**
26. Sorgen Sie auf der Seite *Wählen Sie aus, was auf diesen Computer übertragen werden soll* dafür, dass nur das Benutzerkonto *Don_Hall* ausgewählt ist, und klicken Sie dann auf *Übertragen*. Klicken Sie auf *Schließen*, um den Windows-EasyTransfer-Assistenten zu schließen.
27. Melden Sie sich ab und mit dem Benutzerkonto *Don_Hall* wieder an. Es wird erforderlich sein, für das Konto ein neues Kennwort einzugeben. Verwenden Sie wieder das

Kennwort **P@ssw0rd.** Überprüfen Sie nach der Anmeldung, ob die Datei *Migrationstest.txt* auf dem Desktop vorhanden ist.

Zusammenfassung der Lektion

- Windows-EasyTransfer eignet sich für die Übertragung von Benutzerprofildaten von Computern, auf denen Windows XP, Windows Vista oder Windows 7 verwendet wird, auf Windows 7-Computer.
- Windows-EasyTransfer kann Daten über ein Windows-EasyTransfer-Kabel oder über das Netzwerk vom Quellcomputer auf den Zielcomputer übertragen. Die zu übertragenden Daten lassen sich auch auf einem USB-Wechseldatenträger oder in einer Netzwerkfreigabe speichern.
- USMT 4.0 ist ein Bestandteil des WAIK und wird verwendet, wenn Profildaten von vielen Computern übertragen werden sollen. Mit USMT lassen sich auch Offline-Migrationen durchführen.
- ScanState wird auf dem Quellcomputer verwendet, LoadState auf dem Zielcomputer.
- USMT steuert mit XML-Konfigurationsdateien wie *MigApp.xml*, *MigUser.xml*, *MigDocs.xml* und *Config.xml*, welche Daten vom Quellcomputer auf den Zielcomputer übertragen werden.
- Zur Offline-Migration ist es erforderlich, den Quellcomputer in Windows PE zu starten, damit sich ScanState ausführen lässt.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 3, »Verwalten von Benutzerprofilen«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welches der folgenden Betriebssysteme unterstützt eine Offline-Migration mit USMT?
   A. Windows 2000 Professional
   B. Windows XP Professional
   C. Windows Vista
   D. Windows 7
2. Mit welchem der folgenden Hilfsmittel können Sie Verschlüsselungszertifikate der Benutzer von einem Computer, auf dem Windows XP Professional verwendet wird, auf Windows 7 Professional übertragen? (Wählen Sie alle zutreffenden Antworten.)
   A. Assistent zum Übertragen von Dateien und Einstellungen
   B. USMT
   C. Windows-EasyTransfer
   D. *RoboCopy.exe*

3. Welche XML-Datei teilt ScanState mit, welche Benutzerprofildaten übertragen werden sollen?
   A. *MigDocs.xml*
   B. *MigUser.xml*
   C. *MigApp.xml*
   D. *Config.xml*
4. Was müssen Sie von der Microsoft-Website herunterladen, um USMT 4.0 zu erhalten?
   A. Windows Anytime Upgrade
   B. Windows Upgrade Advisor
   C. WAIK
   D. Microsoft Application Compatibility Toolkit
5. Welcher der folgenden USMT-Migrationsspeichertypen beansprucht am wenigsten Speicherplatz und wird bei Migrationen auf denselben Computer (Wipe-and-Load) verwendet?
   A. Unkomprimiert
   B. Komprimiert
   C. Hard-link

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Windows 7 erfordert einen x86- oder x64-Prozessor mit 1 GHz Taktfrequenz. Die Editionen Starter oder Home Basic setzen mindestens 512 MByte Arbeitsspeicher voraus, die anderen Editionen 1 GByte. Für die Verwendung der Benutzeroberfläche Aero ist außerdem eine Grafikkarte mit mindestens 128 MByte Grafikspeicher Voraussetzung.
- Windows 7 kann in Dual-Boot-Konfigurationen mit Windows XP und Windows Vista verwendet werden. Dabei wird jedes Betriebssystem, das nicht von einer VHD gestartet wird, in einer separaten Partition installiert.
- Windows 7 kann von einer DVD, einem USB-Speichergerät, einer Netzwerkfreigabe oder von den Windows-Bereitstellungsdiensten installiert werden.
- Der Upgrade Advisor kann Sie darüber informieren, welche an Ihrem Windows Vista-Computer angeschlossene Hardware und welche installierte Software zu Windows 7 kompatibel ist.
- Eine x86-Version von Windows Vista können Sie nur auf eine x86-Version von Windows 7 aktualisieren und eine x64-Version von Windows Vista nur auf eine x64-Version von Windows 7.
- Windows XP können Sie nicht direkt auf Windows 7 aktualisieren. Nur Windows Vista lässt sich auf Windows 7 aktualisieren.
- Windows-EasyTransfer ermöglicht die Migration von Benutzerprofildaten von Windows XP- und Windows Vista-Computern auf Windows 7-Computer. Es eignet sich gut für die Migration, wenn nur eine kleine Anzahl von Computern migriert werden muss.
- USMT ist ein Befehlszeilentool, das die Übertragung von Benutzerprofildaten von Windows XP- und Windows Vista-Computern auf Windows 7-Computer ermöglicht. Es eignet sich für eine größere Anzahl von Computern.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Dual-Boot**
- **Netbook**
- **Side-by-Side-Migration**
- **Wipe-and-Load-Migration**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie Ihr Wissen zu den Themen dieses Kapitels an. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: Installieren von Windows 7 bei Contoso

Sie arbeiten für die Firma Contoso. Sie verfügt über eine Zentrale und zwei Zweigstellen. Die Firma hat gerade 50 kleine Laptops erworben, auf denen Sie Windows 7 bereitstellen sollen. 40 dieser Computer sollen in der Zentrale eingesetzt werden und jeweils 5 in den Zweigstellen. Die kleinen Computer sind nicht mit DVD-Laufwerken ausgestattet, verfügen aber über PXE-konforme Netzwerkkarten und USB-Anschlüsse. Sie haben die Windows PE-Standardversion aus dem WAIK getestet und dabei festgestellt, dass sie nicht zu den Netzwerkkarten dieser Computer kompatibel ist. Contoso hat einen Volumenlizenzvertrag mit Microsoft abgeschlossen. Auf allen Servern von Contoso wird das Betriebssystem Windows Server 2008 verwendet. Sie möchten sicherstellen, dass die Festplatten der Computer verschlüsselt sind, damit die Daten auch im Fall eines Verlustes eines oder mehrerer Computer geschützt bleiben. Beantworten Sie nun folgende Fragen:

1. Welches Installationsmedium oder welche Installationsquelle wählen Sie für die Installation von Windows 7 in der Zentrale?
2. Welches Installationsmedium oder welche Installationsquelle wählen Sie für die Bereitstellung von Windows 7 in den Zweigstellen?
3. Welche Edition von Windows 7 sollten Sie auf den Computern installieren?

Übung 2: Migrieren von Benutzerdaten bei Fabrikam

Sie sind bei der Firma Fabrikam für die Clientbetriebssysteme zuständig. In der Zentrale arbeiten 20 Benutzer an Computern, auf denen Windows 7 Enterprise (x86) installiert ist. Sie möchten diese Computer von 4 GByte Arbeitsspeicher auf 16 GByte aufrüsten und müssen das Betriebssystem auf Windows 7 Enterprise (x64) aktualisieren. Nach dem Abschluss der Aktualisierung sollen die Benutzer die x86-Version von Windows 7 nicht mehr starten können. In einer Zweigstelle arbeiten 10 Benutzer noch unter Windows XP Professional an Computern, die älter als 5 Jahre sind. Diese Computer verfügen jeweils nur über 256 MByte Arbeitsspeicher. Sie haben keine Windows-EasyTransfer-Kabel und möchten die Benutzerprofildaten von der Zweigstelle auch nicht auf Netzlaufwerken oder USB-Speichergeräten speichern. Sie ersetzen diese Computer durch 10 neue Computer, auf denen Windows 7 Professional installiert ist. Beantworten Sie nun folgende Fragen:

1. Welche Art von Migration sollten Sie in der Zweigstelle durchführen, Side-by-Side oder Wipe-and-Load?
2. Welche Art von Migration sollten Sie in der Zentrale durchführen, Side-by-Side oder Wipe-and-Load?
3. Mit welcher Technologie und welcher Methode führen Sie die Migrationen in der Zweigstelle durch?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Durchführen einer Neuinstallation

Beschäftigen Sie sich nicht nur mit der reinen Neuinstallation von Windows 7 auf Computern, auf denen noch kein Betriebssystem installiert ist, es kommt auch eine Dual-Boot-Konfiguration mit einem vorhandenen Betriebssystem und Windows 7 in Betracht.

- Konfigurieren Sie einen Computer, auf dem Windows XP oder Windows Vista verwendet wird, so, dass sich wahlweise auch Windows 7 starten lässt. Sorgen Sie dafür, dass Sie eine separate Partition mit mindestens 15 GByte freiem Speicherplatz zur Verfügung haben.

Aktualisieren einer älteren Windows-Version auf Windows 7

Mit dem Windows 7 Upgrade Advisor können Sie überprüfen, ob die Anwendungen und die Hardware eines Computers, auf dem Windows Vista verwendet wird, zu Windows 7 kompatibel sind.

- Laden Sie unter Windows Vista den Windows 7 Upgrade Advisor herunter. Starten Sie den Advisor, um zu überprüfen, ob sich die Hardware des Windows Vista-Computers und die darauf installierte Software für Windows 7 eignen.

Migrieren der Benutzerprofile

Der USMT ist ein umfassendes und komplexes Migrationsprogramm für Benutzerprofile. Wie Windows-EasyTransfer eignet sich auch USMT für die Übertragung der Benutzerprofile von Computern, auf denen Windows XP, Windows Vista oder Windows 7 verwendet wird, auf Windows 7-Computer.

- Erstellen Sie auf dem Computer *Canberra*, auf dem Windows 7 verwendet wird, ein neues Benutzerkonto. Melden Sie sich an und erstellen Sie ein Beispieldokument. Übertragen Sie dieses Konto samt Benutzerprofildaten auf einen anderen Windows 7-Computer. Überprüfen Sie, ob auch das Dokument übertragen wurde.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

K A P I T E L 2

Konfigurieren von Systemabbildern

Als Netzwerkexperte in einer Unternehmensumgebung haben Sie wahrscheinlich schon einmal einen Referenzcomputer konfiguriert, ein Abbild erstellt und dieses Abbild über einen Distributionsserver auf Clientcomputer verteilt. Sie sollten mit dem Tool Sysprep vertraut sein und wissen, wie Sie hardwarespezifische Informationen aus einem Abbild entfernen. Dieses Kapitel beschreibt die Entwicklungen und Verbesserungen der letzten Zeit an den verschiedenen Tools, mit denen Sie *Systemabbilder* (Datenträgerabbilddateien, die ein Betriebssystem enthalten) konfigurieren. Insbesondere geht das Kapitel auf die Verwendung von dateibasierten Windows-Abbildern (Windows Image, WIM) und des Tools ImageX ein.

In älteren Microsoft-Betriebssystemen war die Verwendung von *virtuellen Festplatten* (Virtual Hard Disk, VHD), die Systemabbilder enthielten, auf die Virtualisierung beschränkt. Sie wurden in Kombination mit Software wie Hyper-V, Microsoft Virtual Server und Microsoft Virtual PC eingesetzt, um virtuelle Computer zu implementieren. In Windows 7 wurde diese Möglichkeit erweitert, sodass Sie nun VHDs auf Hardware-PCs erstellen und benutzen können, die keine virtuellen Computer sind. In den Windows 7-Editionen Enterprise und Ultimate können Sie von VHD starten, eine gesamte Systemfestplatte auf VHD sichern und ein Systemabbild auf VHD installieren. Dank dieses neuen Betriebssystemfeatures können Sie das System nach einem Totalausfall des Systemdatenträgers schnell wiederherstellen und einen Failoverschutz implementieren, ohne dafür RAID-Systeme implementieren zu müssen.

Dieses Kapitel beschreibt, wie Sie ein Systemabbild aufzeichnen und es für die Verteilung auf andere Computer vorbereiten. Außerdem erfahren Sie, wie Sie eine VHD so konfigurieren, dass sie ein Systemabbild enthält, und wie Sie einen Computer mit Windows 7 Enterprise oder Ultimate so einrichten, dass er von einer VHD startet, die ein Systemabbild enthält. Das Kapitel stellt die verschiedenen Tools und Methoden vor, mit denen Sie Systemabbilder für die Aufzeichnung vorbereiten und VHD-Dateien verwalten.



Prüfungstipp

Die Verwendung nativer VHDs auf nichtvirtuellen Computern ist ein neues Feature in Windows 7, das mit hoher Wahrscheinlichkeit in der Prüfung 70-680 behandelt wird.

In diesem Kapitel abgedeckte Prüfungsziele:

- Aufzeichnen eines Systemabbilds
- Konfigurieren einer VHD

Lektionen in diesem Kapitel:

- Lektion 1: Aufzeichnen von Systemabbildern 55
- Lektion 2: Verwalten von virtuellen Festplatten 88

Bevor Sie beginnen

Um die Übungen in diesem Kapitel durchzuarbeiten, müssen Sie folgende Vorbereitungen getroffen haben:

- Sie haben Windows 7 auf einem eigenständigen Client-PC installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben. Sie brauchen Internetzugriff, um die Übungen durchzuführen.
- Sie haben eine zweite Festplatte auf diesem Computer bereitgestellt, auf der die VHD abgelegt wird, die Sie erstellen (dies ist optional). Sie können eine interne Festplatte verwenden, sofern eine zur Verfügung steht, oder eine externe Festplatte, beispielsweise ein USB-Gerät. Auf dieser Festplatte sollten mindestens 20 GByte frei sein. Das ist allerdings nicht zwingend nötig, weil Sie eine VHD auch auf dem Laufwerk C: anlegen können; die Übungen werden dadurch aber realistischer.
- Sie brauchen ein USB-Flashlaufwerk (USB Flash Drive, UFD) mit 4 GByte freiem Speicher.

Praxistipp

Ian McLean

Eine größere Anzahl Computer einzurichten, ist viel einfacher geworden als noch vor 10 oder 5 Jahren.

Ich erinnere mich noch, wie ich von Computer zu Computer ging, jeden von einer Diskette startete, auf der ein Teil von MS-DOS implementiert war, der Netzwerkzugriff und Dateiübertragung ermöglichte (aber kaum etwas anderes). Dann wurden Installationsdateien und Antwortdateien auf jeden Clientcomputer geladen (oft aus einem einzigen, schmerzhaft langsamen CD-Laufwerk) und das Betriebssystem wurde installiert. In jenen Tagen war der Begriff »unbeaufsichtigte Installation« ein Scherz. Ich weiß noch, wie ich mitten in der Nacht meine Runde bei mehreren Hundert Computern machte, nur um zu bestätigen, dass wir die Lizenzbedingungen akzeptierten.

Die Installation aufgezeichneter Abbilder hatte andere Schwierigkeiten in petto. Üblicherweise mussten Sie dabei für jeden Computer ein anderes Abbild aufzeichnen, damit die Sicherheits-IDs unterschiedlich waren. Das war keine große Sache für Trainingsnetzwerke, wo Sie für jeden Kurs andere Abbilder brauchten. Aber wenn Hunderte neuer Computer installiert werden mussten, war das einfach nicht akzeptabel. Sysprep wurde daher schon sehnlich erwartet, als es eingeführt wurde. Wenn Sie ein Abbild aufzeichneten, dessen Daten nur eine begrenzte Lebensdauer hatten (zum Beispiel Kennwörter), es aber erst später anwendeten, lauerten überall Probleme. Ich habe noch lebhaft in Erinnerung, wie ich einen Computer aus einem Abbild als Domänencontroller für einen Microsoft-Kurs installierte und feststellen durfte, dass 1.000 Kennwörter abgelaufen waren. Und wenn man ein Abbild von einem Computer anfertigte und dieses Abbild später installierte, wurde keines der Sicherheitsupdates eingespielt, die in der Zwischenzeit erschienen waren, sodass der Computer anfangs verwundbar war.

Inzwischen können Clientcomputer aus Abbilddateien installiert werden, die auf einem Distributionsserver liegen (das geht viel schneller, als Installationsdateien herunterzuladen und auszuführen). Abbilder können verallgemeinert werden, indem SIDs und

Computernamen entfernt werden. Sie können Sicherheitsupdates, Language Packs und Anwendungen zu einem Abbild hinzufügen, bevor Sie es verteilen, und Sie können Ihre Abbilder auf dem neusten Stand halten.

Das Leben eines Administrators ist nicht einfach. Aber ich denke, es ist ein bisschen besser als früher. Machen Sie sich mit den optimalen Möglichkeiten vertraut, sehr viele Clientcomputer auf einmal zu installieren. Es macht einen Teil Ihrer Arbeit deutlich einfacher. Und für die Prüfung schadet es garantiert auch nicht!

Lektion 1: Aufzeichnen von Systemabbildern

Diese Lektion beschreibt, wie Sie ein Systemabbild für die automatisierte oder manuelle Aufzeichnung vorbereiten und wie Sie Windows-Abbilddateien (Windows Image, WIM) bearbeiten. Es stellt das Windows Automated Installation Kit (Windows AIK), das Windows Preinstallation Environment (Windows PE) und das Befehlszeilentool Sysprep vor.

Die Lektion geht kurz auf das Microsoft Deployment Toolkit (MDT) 2010 und das Tool DISM (Deployment Image Servicing and Management) ein. Kapitel 3, »Bereitstellen von Systemabbildern«, beschreibt im Anschluss genauer, wie Sie mithilfe von DISM Systemabbilder erweitern und wie Sie MDT laden, installieren und damit ein Systemabbild bereitstellen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Herunterladen und Verwenden des Windows AIK; im Einzelnen die Verwendung der Tools ImageX und Oscdimg, um Systemabbilder zu erstellen, und die Benutzung des Windows System Image Managers (System Image Manager, SIM), um eine Antwortdatei zu erstellen, die eine unbeaufsichtigte Installation eines WIM-Abbilds ermöglicht
- Erstellen eines Windows PE-Startdatenträgers, Starten mit Windows PE und Erstellen eines Abbilds für eine Windows 7-Installation
- Vorbereiten eines Referenzcomputers für die Abbilderstellung mit dem Tool Sysprep und Beschreiben der Windows-Setup-Konfigurationsphasen
- Beschreiben der Funktionen des Tools MDT und wie Sie mit der Deployment Workbench auf die MDT-Dokumentation zugreifen, die erklärt, welche Schritte Sie durchführen müssen, bevor Sie ein Betriebssystem bereitstellen (Kapitel 3 beschreibt dieses Tool im Detail.)

Veranschlagte Zeit für diese Lektion: 50 Minuten

Installieren und Benutzen des Windows Automated Installation Toolkit

Das *Windows Automated Installation Kit* (Windows AIK) ist eine Sammlung von Tools und dazugehöriger Dokumentation, die Ihnen dabei hilft, Abbilder des Betriebssystems Microsoft Windows auf Zielcomputern oder einer VHD bereitzustellen. Sie können das Windows AIK benutzen, um Windows 7-Installationen zu automatisieren, Windows-Systemabbilder mit ImageX aufzuzeichnen, Abbilder mit DISM zu konfigurieren und zu bearbeiten, Windows PE-Abbilder zu erstellen und Benutzerprofile sowie -daten mit dem User State Migration Tool (USMT) zu migrieren.

Das Windows AIK umfasst mehrere Tools, mit denen Sie verschiedene Bereitstellungsoptionen konfigurieren. Abhängig von Ihren Anforderungen brauchen Sie nur einige der Ressourcen oder alle, die im Windows AIK zur Verfügung stehen.

Sie installieren das Windows AIK, indem Sie erst das ISO-Abbild herunterladen, es auf eine DVD brennen und dann von dieser DVD installieren. Zu dem Zeitpunkt, als dieses Kapitel geschrieben wurde, konnte man das ISO-Abbild mit dem Windows AIK herunterladen, indem man *http://technet.microsoft.com/de-de/library/dd349343.aspx* aufrief und den entsprechenden Link anklickte.

Installieren des Windows AIK von einer DVD

Eine Installations-DVD erstellen Sie, indem Sie das heruntergeladene ISO-Abbild auf einen DVD-Rohling brennen. Klicken Sie mit der rechten Maustaste auf die ISO-Abbilddatei und wählen Sie den Befehl *Datenträgerabbild brennen*. Gehen Sie folgendermaßen vor, um das Windows AIK von DVD zu installieren:

1. Legen Sie die DVD ein. Klicken Sie auf der Seite *Willkommen* auf *Windows AIK-Setup*.
2. Klicken Sie auf der Seite *Willkommen* des Setup-Assistenten auf *Weiter*.
3. Wählen Sie die Option *Ich stimme zu* aus, um die Lizenzbedingungen anzunehmen. Klicken Sie auf *Weiter*.
4. Klicken Sie auf der Seite *Installationsordner auswählen* auf *Weiter*, um die Standardeinstellung zu übernehmen (sofern Sie den Installationsordner nicht ändern wollen).
5. Klicken Sie auf *Weiter*, um die Installation zu starten. Die Installation kann einige Zeit dauern.
6. Klicken Sie auf *Schließen*.

Sobald das Windows AIK installiert ist, können Sie es im Menü *Alle Programme* öffnen. So erhalten Sie Zugriff auf die Windows AIK-Dokumentation, auf die Eingabeaufforderung für Bereitstellungstools, die Ihnen Zugriff auf Befehlszeilenprogramme wie ImageX, DISM und das Tool Oscdimg (zum Erstellen von ISO-Abbildern) bietet, und auf Windows SIM.

Schnelltest

- Welches Windows AIK-Tool verwenden Sie, um eine Antwortdatei zu erstellen, mit der Sie eine unbeaufsichtigte Installation eines WIM-Abbilds ausführen?

Antwort zum Schnelltest

- Windows SIM

Windows AIK-Tools

Tabelle 2.1 listet die Tools auf, die im Windows AIK enthalten sind.

Tabelle 2.1 Im Windows AIK enthaltene Tools

Tool	Beschreibung
Windows SIM	Öffnet Windows-Abbilder, erstellt Antwortdateien und verwaltet Bereitstellungsfreigaben und Konfigurationssätze.
ImageX	Dient zum Aufzeichnen, Erstellen, Bearbeiten und Anwenden von Windows-Abbildern.
DISM	Wendet Updates, Treiber und Language Packs auf ein Windows-Abbild an. DISM steht in allen Installationen von Windows 7 zur Verfügung.
Windows PE-Tools	Das Windows AIK enthält mehrere Tools, die dazu dienen, Windows PE-Umgebungen aufzubauen und zu konfigurieren.
USMT	Zum Migrieren von Benutzerdaten aus einer älteren Windows-Version auf Windows 7. USMT wird als Teil des Windows AIK im Verzeichnis *%ProgramFiles%\Windows AIK\Tools\USMT* installiert.
Oscdimg	Erstellt ISO-Abbilder.



Weitere Informationen USMT

Weitere Informationen über USMT finden Sie im Benutzerhandbuch zum User State Migration Tool. Wenn Sie Windows AIK und USMT installieren, befindet sich dieses Handbuch im Pfad *%ProgramFiles%\Windows AIK\Docs\Usmt.chmz*.

Arbeiten mit Windows PE

Die Windows-Vorinstallationsumgebung (Windows Preinstallation Environment Version 3.0, meist kurz *Windows PE* genannt) ist eine schlanke Windows 7-Version, die in erster Linie für die Bereitstellung von Clientcomputern eingesetzt wird. Windows PE ist als 32-Bit- oder 64-Bit-Ersatz für MS-DOS gedacht, der während der Installationsphase von Windows 7 zum Einsatz kommt. Es kann über PXE (Preboot Execution Environment), DVD, UFD, VHD oder Festplatte gestartet werden. Windows PE steht kostenlos im Windows AIK zur Verfügung.

Ursprünglich wurde Windows PE als Vorinstallationsplattform zum Bereitstellen von Windows-Betriebssystemen benutzt. Es hat sich seitdem zu einer Plattform weiterentwickelt, in der Sie in einer Unternehmensumgebung Arbeitsstationen und Server bereitstellen, sowie zu einer Wiederherstellungsplattform, in der Sie 32-Bit- oder 64-Bit-Wiederherstellungstools wie die Windows-Wiederherstellungsumgebung (Windows Recovery Environment, Windows RE) ausführen.

Üblicherweise verwenden Sie das Skript *Copype.cmd* aus dem Unterverzeichnis *C:\Program Files\Windows AIK\Tools\PETools*, um ein lokales Windows PE-Buildverzeichnis anzulegen. Dann erstellen Sie mit dem Windows AIK-Tool Oscdimg aus demselben Unterverzeichnis ein ISO-Abbild von Windows PE 3.0. Mit diesem Abbild erstellen Sie schließlich eine startfähige DVD. Nun können Sie von der DVD die Pre-Boot-Umgebung starten und dort mit dem Tool ImageX ein WIM-Abbild aufzeichnen. Diese Schritte arbeiten Sie in den Übungen am Ende dieser Lektion durch.

Erstellen eines Referenzabbilds

Weiter unten in diesem Kapitel wird beschrieben, wie Sie mit dem Windows AIK-Tool ImageX und Windows PE ein WIM-Abbild eines Computers mit Windows 7 Enterprise oder Ultimate vorbereiten und dieses Abbild in eine startfähige VHD auf demselben Computer schreiben, sodass Sie das Abbild von der VHD starten können. Auf diese Weise erhalten Sie Schutz für den Fall, dass bei diesem Computer ein Fehler auftritt; das Abbild dient auch als eine Art Datensicherung. Diese Schritte führen Sie in den Übungen in dieser Lektion und in Lektion 2 dieses Kapitels durch.

In einer Unternehmensumgebung werden Sie allerdings Windows 7 eher auf einem Referenzcomputer installieren und dann ein Abbild davon erstellen, das Sie auf beliebig vielen Clientcomputern in Ihrem Netzwerk installieren. Kapitel 3 beschreibt, wie Sie die neusten Sicherheitsupdates für das Betriebssystem, wichtige Anwendungen und Language Packs zu einem aufgezeichneten Abbild hinzufügen.



Prüfungstipp

Wenn Sie ein Abbild Ihres aktuellen Windows 7-Computers aufzeichnen und das Abbild in einer VHD speichern wollen, von der Sie den Computer starten können, muss Windows 7 Enterprise oder Ultimate auf dem Computer installiert sein. Wenn Sie allerdings einen Referenzcomputer aufgebaut haben und ein Systemabbild dieses Computers erstellen wollen, um es auf mehrere Zielcomputer zu verteilen, können Sie eine beliebige Windows 7-Edition verwenden, um das Abbild für die Verteilung zu erstellen.

Sie müssen ein Referenzabbild verallgemeinern, hardwarespezifische Informationen deinstallieren (beispielsweise die SID des Referenzcomputers) und eine Installationsantwortdatei sowie Skripts zum Automatisieren der Installation generieren.

Neben dem Referenzcomputer, dessen Abbild Sie zusammenstellen und aufzeichnen, brauchen Sie im Allgemeinen auch noch einen Administrationscomputer, auf dem die Tools laufen, mit denen Sie das Abbild verallgemeinern und aufzeichnen, zum Beispiel die Windows AIK-Tools. Dieser Administrationscomputer braucht nicht unter Windows 7 zu laufen, Sie können dafür auch einen Windows Vista- oder Windows XP-Client verwenden.

Der Ablauf für die Installation des Windows AIK auf dem Administrationscomputer wurde im letzten Abschnitt beschrieben. Gehen Sie folgendermaßen vor, um einen Referenzcomputer zu konfigurieren und ein Abbild aufzuzeichnen, das sich für die Verteilung auf Ihre Clientcomputer eignet:

1. Erstellen Sie eine Antwortdatei, mit der Sie die Installation von Windows 7 auf dem Referenzcomputer automatisieren (als Option).
2. Überprüfen und speichern Sie Ihre Einstellungen.
3. Konfigurieren Sie eine Referenzinstallation.
4. Erstellen Sie eine startfähige Windows PE-DVD oder -UFD, die das Windows AIK-Tool ImageX enthält.
5. Zeichnen Sie die Installation in einer Netzwerkfreigabe auf.
6. Stellen Sie das Abbild in einer Netzwerkfreigabe bereit.



Hinweis Verwenden einer Antwortdatei

Sie brauchen nicht zwingend eine Antwortdatei zu erstellen, auch wenn diese Methode in der Microsoft-Dokumentation empfohlen wird. Wenn Sie möchten, können Sie den Referenzcomputer auch von Hand installieren.

Bauen einer Antwortdatei

Der erste (optionale) Schritt beim Erstellen einer maßgeschneiderten Installation auf Ihrem Referenzcomputer besteht darin, auf Ihrem Administrationscomputer eine Antwortdatei zu erstellen, mit der Sie die Windows-Einstellungen während der Installation konfigurieren. Sie können beispielsweise die Standardeinstellungen für den Windows Internet Explorer konfigurieren, das Netzwerk einrichten und andere Anpassungen vornehmen. Die Antwortdatei sollte alle Einstellungen enthalten, die für eine unbeaufsichtigte Installation gebraucht werden, sodass während der Installation keine Benutzeroberflächenseiten erscheinen, in denen Sie Eingaben vornehmen müssen. Wenn Sie wollen, können Sie den Referenzcomputer allerdings auch mit der herkömmlichen Methode einrichten, also durch »Mausklicken und Eintippen«.

Mit dem Tool Windows SIM aus dem Windows AIK erstellen Sie auf Ihrem Administrationscomputer eine Antwortdatei, die die grundlegende Windows Setup-Konfiguration und einige Anpassungen für die Windows-Willkommensseiten enthält. In diesem Beispiel importiert die Antwortdatei keine speziellen Treiber, Anwendungen oder Pakete. Komplexere Antwortdateien lernen Sie in Kapitel 3 kennen.



Hinweis Beispielantwortdatei

Wenn Sie das Windows AIK auf Ihrem Administrationscomputer installieren, wird eine Beispielantwortdatei namens *Corp_autounattended_sample.xml* im Ordner *C:\Program Files\Windows AIK\Samples* installiert.

Sie erstellen eine Antwortdatei, indem Sie eine Windows-Abbilddatei (Windows Image, WIM) auf Ihren Administrationscomputer kopieren und dann das Tool Windows SIM starten. Gehen Sie folgendermaßen vor, um eine Antwortdatei zu erstellen, mit der Sie Windows 7 aus der WIM-Datei, die auf der Installations-DVD enthalten ist, auf Ihrem Referenzcomputer installieren:

1. Erstellen Sie auf Ihrem Administrationscomputer einen Ordner namens *C:\Myimages*.
2. Legen Sie die Windows 7-Produkt-DVD in Ihren Administrationscomputer ein.
3. Wechseln Sie in das Verzeichnis *\Sources* Ihres DVD-Laufwerks und kopieren Sie die Datei *Install.wim* von der Windows-Produkt-DVD in *C:\Myimages*.
4. Klicken Sie im Startmenü auf *Alle Programme*, *Microsoft Windows AIK* und dann auf *Windows System Image Manager*. Daraufhin wird Windows SIM gestartet.
5. Klicken Sie im Fensterabschnitt *Windows-Abbild* von Windows SIM mit der rechten Maustaste auf *Windows-Abbild oder Katalogdatei auswählen* und wählen Sie den Befehl *Windows-Abbild auswählen* (Abbildung 2.1).

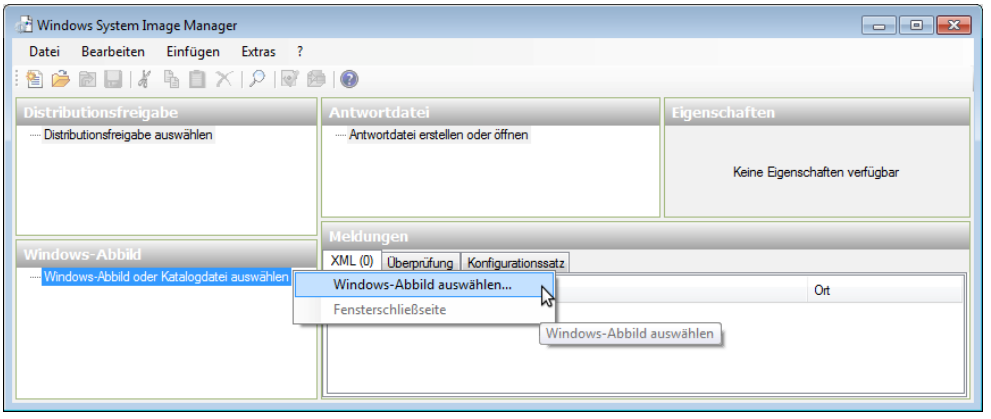


Abbildung 2.1 Auswählen eines Windows-Abbilds

6. Wechseln Sie im Dialogfeld *Windows-Abbild auswählen* zum Ordner *C:\Myimages*, wählen Sie die Datei *Install.wim* aus und klicken Sie auf *Öffnen*.
7. Sie werden im Dialogfeld *Abbild auswählen* aufgefordert, das Abbild auszuwählen, das Sie installieren wollen. Wählen Sie das gewünschte Abbild (zum Beispiel *Windows 7 Ultimate*) und klicken Sie auf *OK*.
8. Klicken Sie auf *Ja*, falls Sie gefragt werden, ob eine Katalogdatei erstellt werden soll. Klicken Sie bei Bedarf noch einmal auf *Ja*, um die Ausführung des Programms zu erlauben. Es kann einige Zeit dauern, eine Katalogdatei zu erstellen.
9. Wählen Sie im Menü *Datei* den Befehl *Neue Antwortdatei*. Daraufhin wird im Fensterabschnitt *Antwortdatei* eine leere Antwortdatei mit dem Namen *Untitled* aufgelistet (Abbildung 2.2).

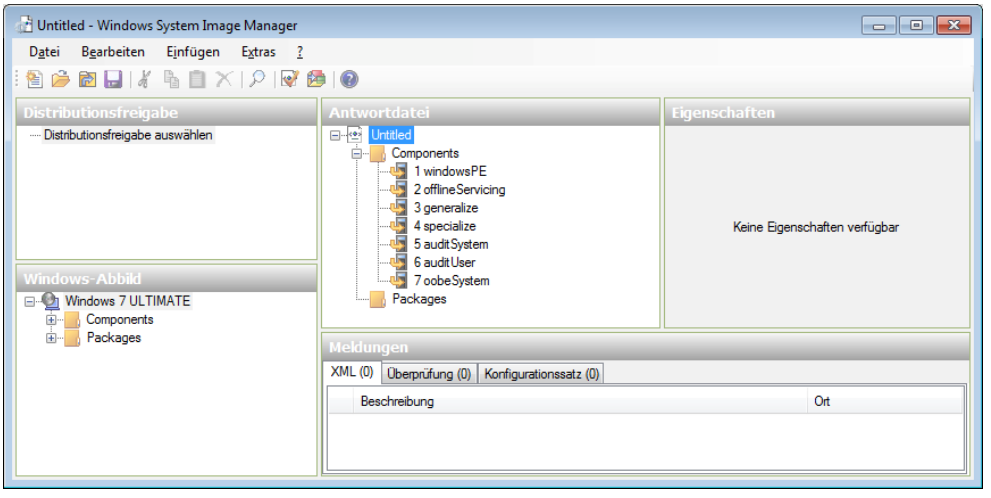


Abbildung 2.2 Erstellen einer leeren Antwortdatei

10. Erweitern Sie im Fensterabschnitt *Windows-Abbild* den Knoten *Components*, damit alle verfügbaren Featureeinstellungen sichtbar sind.
11. Fügen Sie in der erweiterten Liste die gewünschten Features zu Ihrer Antwortdatei hinzu, indem Sie jeweils mit der rechten Maustaste auf ein Feature klicken und den entsprechenden Konfigurationsdurchlauf (*Pass*) auswählen. Tabelle 2.2 zeigt einen grundlegenden Satz Features mit dem zugehörigen Konfigurationsdurchlauf. Wählen Sie jeweils den passenden Konfigurationsdurchlauf aus (Abbildung 2.3)

Tabelle 2.2 Verfügbare Features und ihr zugehöriger Konfigurationsdurchlauf

Feature	Konfigurations-durchlauf
x86_Microsoft-Windows-Deployment_6.1.<*Build*>_neutral	*oobeSystem*
x86_Microsoft-Windows-International-Core-WinPE_6.1.<*Build*>_neutral	*windowsPE*
x86_Microsoft-Windows-Setup_6.1.<*Build*>_neutral	*windowsPE*
x86_Microsoft-Windows-Shell-Setup_6.1.<*Build*>_neutral	*oobeSystem*

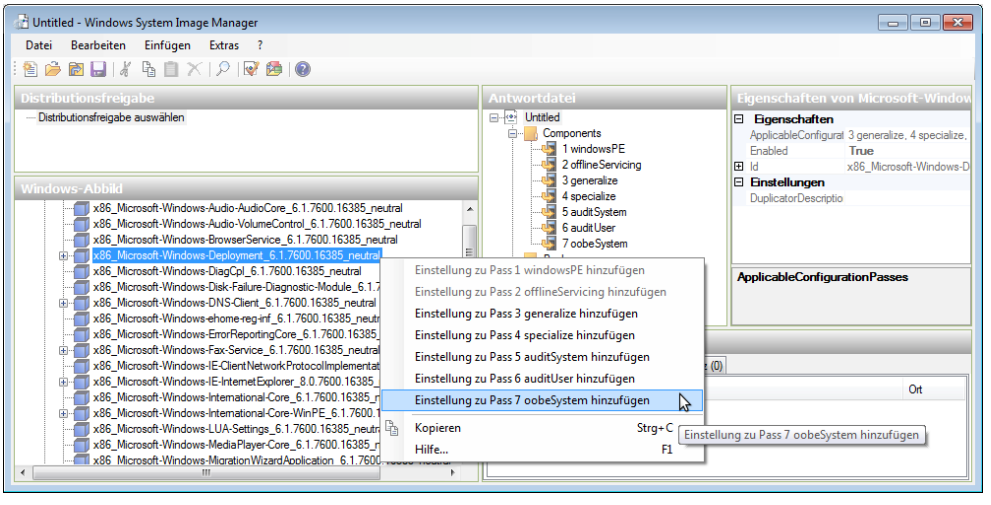


Abbildung 2.3 Auswählen eines Konfigurationsdurchlaufs (Pass)

12. Wählen Sie im Zweig *Einstellungen* eine Einstellung aus und geben Sie in der rechten Spalte den zugehörigen Wert ein. Typische Werte sehen Sie in Tabelle 2.3 (die Tabelle enthält Beispieleinträge für das Gebietsschema Deutsch/Deutschland). Abbildung 2.4 zeigt die fertigen Einstellungen im Fenster *Windows System Image Manager*.

Tabelle 2.3 Hinzufügen von Einstellungswerten zu Komponenten

Konfigurations-durchlauf	Feature	Wert

WindowsPE	x86_Microsoft-Windows-International-Core-WinPE_ 6.1.<*Build*>_neutral	`InputLocale = de-DE`
		`SystemLocale = de-DE`
		`UILanguage = de-DE`
		`UserLocale = de-DE`

WindowsPE	x86_Microsoft-Windows-Setup_ 6.1.<*Build*>_neutral	`EnableFirewall = true`
		`EnableNetwork = true`
		`LogPath = <Pfad zu Protokolldateien>`
		`Restart = Restart`
		`UseConfigurationSet = true`

oobeSystem	x86_Microsoft-Windows-Deployment_6.1.<*Build*>_ neutral	`Id = x86_Microsoft-Windows-Deployment__neutral_<GUID>_nonSxS`

oobeSystem	x86_Microsoft-Windows-Shell-Setup_6.1.<*Build*>_neutral	`BluetoothTaskbarIconEnabled = true`
		`DisableAutoDaylightTimeSet = false`
		`DoNotCleanTaskBar = true`
		`RegisteredOrganization = Microsoft`
		`RegisteredOwner = Microsoft`
		`ShowWindowsLive = true`
		`StartPanelOff = true`
		`TimeZone = CET`

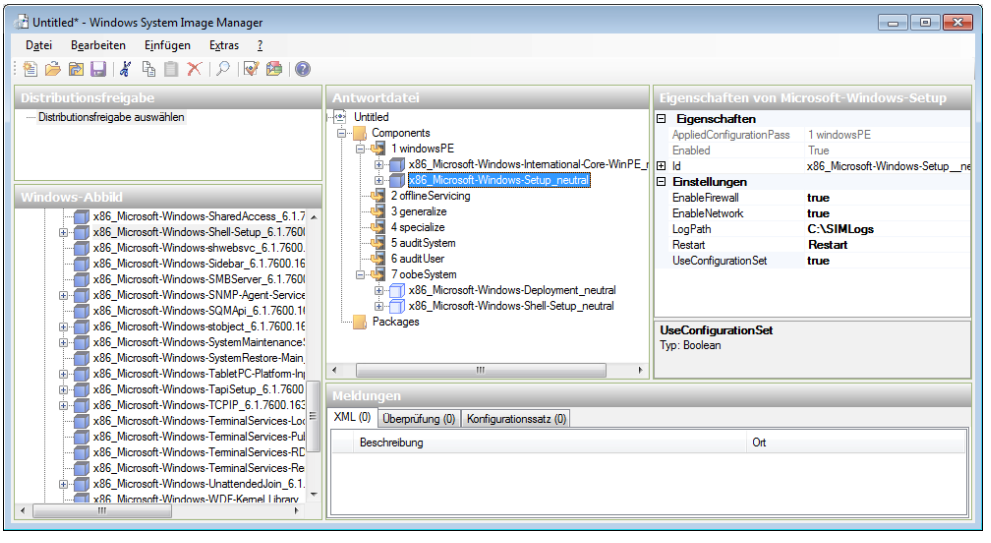


Abbildung 2.4 Einstellungen für Features im Fenster *Windows System Image Manager* (SIM)

13. Wenn Sie möchten, können Sie den Knoten eines Features aufklappen und bei zusätzlichen Sätzen mit Featurewerten die Standardeinstellungen ändern. Abbildung 2.5 zeigt diese Möglichkeit.

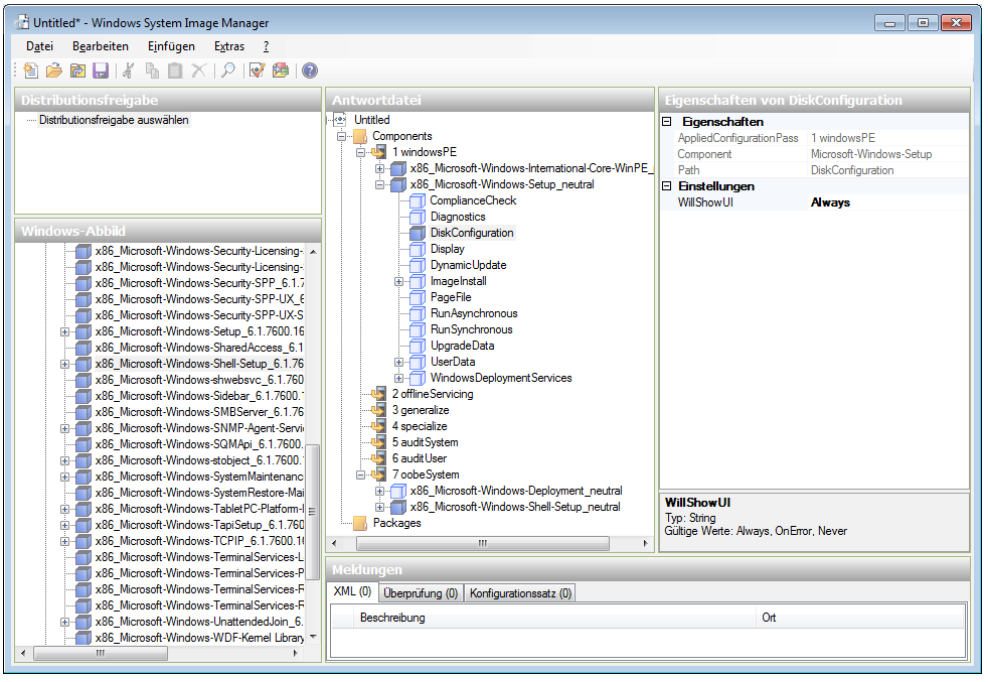


Abbildung 2.5 Ändern der Standardwerte

Diese Einstellungen definieren eine simple unbeaufsichtigte Installation, bei der während des Windows-Setups keine Benutzereingaben vorgenommen werden brauchen. Sobald die Installation abgeschlossen ist, wird der Computer im Überwachungsmodus neu gestartet. Auf diese Weise können Sie schnell den Desktop starten, zusätzliche Anwendungen sowie Gerätetreiber installieren und die Installation testen. Die Windows-Willkommensseite wird im Überwachungsmodus nicht ausgeführt; sie erscheint erst, wenn der Computer das nächste Mal neu gestartet wird, nachdem Sie den Befehl `sysprep /oobe` ausgeführt haben. Die Windows-Willkommensseite (Windows Welcome, intern gelegentlich auch als Machine OOBE bezeichnet) fordert den Benutzer auf, die Microsoft-Softwarelizenzbedingungen zu lesen und den Computer zu konfigurieren.



Weitere Informationen Überwachungsmodus und Sysprep

Weitere Informationen über den Überwachungsmodus finden Sie unter *http://technet.microsoft.com/de-de/library/cc722413.aspx*. Weitere Informationen über das Tool Sysprep enthält *http://technet.microsoft.com/de-de/library/cc766049.aspx*.

Überprüfen und Speichern der Einstellungen

Gehen Sie folgendermaßen vor, um die Einstellungen in Ihrer Antwortdatei zu überprüfen und sie in einer Datei auf einem Wechseldatenträger zu speichern:

1. Klicken Sie in Windows SIM auf *Extras* und wählen Sie den Befehl *Antwortdatei überprüfen*.
2. Warnungen, die darauf hinweisen, dass Standardeinstellungen nicht geändert wurden, verhindern nicht, dass die Datei überprüft oder gespeichert wird. Tauchen dagegen Fehlermeldungen oder andere Benachrichtigungen im Fensterabschnitt *Meldungen* auf, müssen Sie Ihre Einstellungen prüfen.
3. Wird im Fensterabschnitt *Meldungen* ein Fehler angezeigt, können Sie die Fehlermeldung doppelt anklicken, um zur monierten Einstellung zu springen. Ändern Sie die Einstellung, um den Fehler zu beseitigen, und führen Sie dann erneut eine Überprüfung durch, indem Sie den Menübefehl *Extras/Antwortdatei überprüfen* wählen. Wiederholen Sie diesen Schritt, bis die Antwortdatei fehlerfrei ist.
4. Wählen Sie im Menü *Datei* den Befehl *Antwortdatei speichern*. Geben Sie der Antwortdatei den Namen *Autounattend.xml*. Abbildung 2.6 zeigt einen Ausschnitt aus einer solchen Datei.

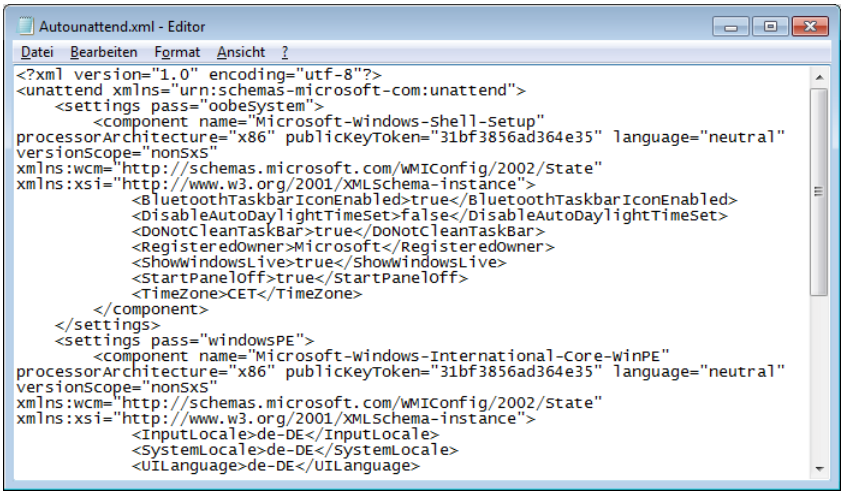


Abbildung 2.6 Eine *Autounattend.xml*-Datei

5. Kopieren Sie die Datei *Autounattend.xml* in das Stammverzeichnis eines Wechselmediengeräts (etwa eines UFD, USB-Flash-Laufwerks). Sie verfügen nun über eine einfache Antwortdatei, die das Windows-Setup automatisiert.



Weitere Informationen **Erstellen von Antwortdateien**

Weitere Informationen, wie Sie Antwortdateien erstellen, enthält *http://technet.microsoft.com/de-de/library/cc748874.aspx*. Diese Seiten behandeln Windows Vista, die Informationen gelten aber genauso für Windows 7.

Erstellen einer Referenzinstallation

Sie konfigurieren Ihren Referenzcomputer mit einer angepassten Installation von Windows 7, die Sie anschließend auf die Zielcomputer kopieren. Eine Referenzinstallation richten Sie mithilfe der Windows-Produkt-DVD und (optional) der Antwortdatei ein, die Sie im vorherigen Abschnitt erstellt haben. Gehen Sie folgendermaßen vor, um Ihren Referenzcomputer mithilfe einer Antwortdatei zu installieren:

1. Schalten Sie den Referenzcomputer ein. Legen Sie die Windows 7-Produkt-DVD ein und stecken Sie das UFD an, auf dem Sie die im vorherigen Abschnitt erstellte Antwortdatei (*Autounattend.xml*) gespeichert haben. Beachten Sie, dass Sie nicht zwingend eine Antwortdatei verwenden müssen, auch wenn Microsoft diese Methode empfiehlt. Wenn Sie möchten, können Sie Windows 7 stattdessen auch manuell von der Produkt-DVD installieren.
2. Starten Sie den Computer neu, indem Sie die Tastenkombination STRG+ALT+ENTF drücken. Unter Umständen müssen Sie die Startreihenfolge im BIOS ändern, damit der Computer von CD/DVD startet. Drücken Sie in diesem Fall während des ersten Systemstarts die entsprechende Funktionstaste, um die Startreihenfolge zu ändern. Windows Setup (*Setup.exe*) startet automatisch und sucht in den Stammverzeichnissen aller Wechseldatenträger nach einer Antwortdatei namens *Autounattend.xml*.
3. Sobald Setup abgeschlossen ist, können Sie überprüfen, ob alle Ihre Anpassungen angewendet wurden. Wenn Sie in Ihrer Antwortdatei beispielsweise das optionale Feature *Microsoft-Windows-IE-InternetExplorer* hinzugefügt und die Einstellung *Home_Page* verändert haben, können Sie diese Einstellungen überprüfen, indem Sie den Internet Explorer öffnen.



Hinweis Installieren einer kleinen Gruppe von Clientcomputern

Wollen Sie nur sehr wenige Clientcomputer installieren (etwa bis zu 5), können Sie die Installation auch einfach auf jedem Computer mithilfe der Produkt-DVD und der Datei *Autounattend.xml* wiederholen. Handelt es sich um mehr Computer, ist es dagegen effizienter, ein WIM-Abbild zu erstellen und es zu verteilen. Dazu müssen Sie den Referenzcomputer für den Benutzer vorbereiten.

4. Wenn Sie den Referenzcomputer für den Benutzer vorbereiten, rufen Sie das Tool Sysprep mit dem Argument `/generalize` auf, um hardwarespezifische Daten aus der Windows-Installation zu entfernen, und mit dem Argument `/oobe`, um den Computer so zu konfigurieren, dass er beim nächsten Neustart die Windows-Willkommensseite anzeigt. Öffnen Sie dazu auf dem Referenzcomputer eine Eingabeaufforderung mit erhöhten Rechten und führen Sie den folgenden Befehl aus:

   c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown

Sysprep bereitet das Abbild für die Aufzeichnung vor, indem es verschiedene benutzer- und computerspezifische Einstellungen beseitigt und Protokolldateien entfernt. Nun ist die Referenzinstallation abgeschlossen, sodass Sie ein Abbild davon anfertigen können.



Vorsicht Out-of-Box-Gerätetreiber

Wenn Sie den Befehl `sysprep /generalize` ausführen, werden Out-of-Box-Gerätetreiber aus dem Windows-Abbild entfernt. Falls Sie während der Installation Out-of-Box-Gerätetreiber hinzufügen und ein Windows-Abbild aufzeichnen wollen, das diese Treiber enthält, müssen Sie in der Antwortdatei beim Feature *Microsoft-Windows-PnpSysprep* die Einstellung `PersistAllDeviceInstalls` auf den Wert `true` setzen.

Erstellen eines startfähigen Windows PE-Mediums

In diesem Schritt erstellen Sie eine startfähige Windows PE-CD oder -DVD. Dafür setzen Sie das Skript *Copype.cmd* ein. Mithilfe von Windows PE können Sie einen Computer für Bereitstellungs- und Wiederherstellungszwecke starten, wobei er ausschließlich aus dem Arbeitsspeicher heraus arbeitet. Sobald der Computer gestartet worden ist, können Sie das Windows PE-Medium wieder entfernen. Wenn Sie den Computer mit Windows PE gestartet haben, können Sie das Tool ImageX aufrufen, um Datenträgerabbilder aufzuzeichnen, zu ändern und anzuwenden.



Hinweis Erstellen eines Abbilds auf VHD mithilfe eines startfähigen Windows PE-Datenträgers

Sie verwenden Windows PE auch, wenn Sie das Abbild eines Computers mit Windows 7 Enterprise oder Ultimate aufzeichnen, um eine startfähige VHD zu installieren. Diesen Vorgang arbeiten Sie in der Übung zu Lektion 2 vollständig durch.



Weitere Informationen Technische Referenz zu den Bereitstellungstools

Weitere Informationen über die Microsoft-Bereitstellungstools finden Sie unter *http://technet.microsoft.com/de-de/library/cc766376.aspx*.

Gehen Sie folgendermaßen vor, um eine startfähige Windows PE-CD oder -DVD zu erstellen und das Windows AIK-Tool ImageX auf diesem Datenträger zu installieren:

1. Legen Sie auf Ihrem Administrationscomputer ein lokales Windows PE-Buildverzeichnis an. Öffnen Sie dann eine Eingabeaufforderung mit erhöhten Rechten und geben Sie die folgenden Befehle ein:

   ```
   cd C:\Program Files\Windows AIK\Tools\PETools\
   copype.cmd <Architektur> <Ziel>
   ```

   Dabei ist *<Architektur>* x86, amd64 oder ia64, und *<Ziel>* ist ein Pfad zu einem lokalen Verzeichnis. Zum Beispiel erstellt der folgende Befehl ein Windows PE-Buildverzeichnis namens *winpe_86* auf einem x86-Computer:

   ```
   copype.cmd x86 C:\winpe_x86
   ```

2. Kopieren Sie ImageX in das Unterverzeichnis *Iso* Ihres Windows PE-Buildverzeichnisses. Auf einem x86-Computer lautet der entsprechende Befehl:

   ```
   copy "C:\Program Files\Windows AIK\Tools\x86\imagex.exe" C:\winpe_x86\iso\
   ```

3. Optional können Sie in einem Texteditor wie dem Windows-Editor eine Konfigurationsdatei namens *Wimscript.ini* erstellen. Diese Konfigurationsdatei weist das Tool

ImageX an, während der Aufzeichnungsoperation bestimmte Dateien (etwa *Pagefile.sys* oder alle *.zip*-Dateien) auszuschließen. Abbildung 2.7 zeigt eine *Wimscript.ini*-Datei.

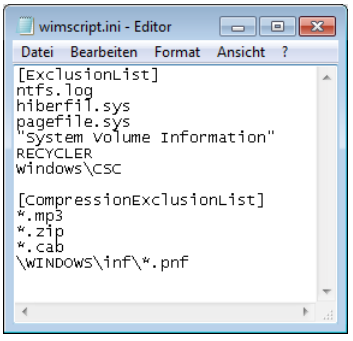


Abbildung 2.7 Eine *Wimscript.ini*-Datei

4. Speichern Sie die Konfigurationsdatei im Unterverzeichnis *Iso* des Windows PE-Buildverzeichnisses. Das Tool ImageX erkennt eine *Wimscript.ini*-Datei, wenn sie sich an diesem Speicherort befindet.



Prüfungstipp

Es gibt keinen Befehl, der ImageX anweist, nach einer *Wimscript.ini*-Datei zu suchen. Das Tool ImageX erkennt *Wimscript.ini* automatisch, sofern sie im selben Ordner wie das Tool selbst gespeichert ist.

5. Erstellen Sie mit dem Tool Oscdimg eine Abbilddatei (*.iso*). Auf einem x86-Computer klicken Sie dazu auf *Alle Programme*, dann auf *Microsoft Windows AIK* und schließlich auf *Eingabeaufforderung für Bereitstellungstools* und geben in der Eingabeaufforderung den folgenden Befehl ein:

   oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso



Weitere Informationen ***Etfsboot.com***

Dieses Argument gibt den Speicherort der El-Torito-Startsektordatei an. Weitere Informationen finden Sie unter *http://technet.microsoft.com/de-de/library/cc749036.aspx*. Beachten Sie außerdem, dass zwischen dem Argument `-b` und dem Pfad *C:\Winpe_x86\Etfsboot.com* kein Leerzeichen stehen darf.

6. Brennen Sie das Abbild (*Winpe_x86.iso*) auf eine CD oder DVD. Sie verfügen nun über einen startfähigen Windows PE-Datenträger, der das Tool ImageX enthält.

Aufzeichnen der Installation in eine Netzwerkfreigabe

Ein Abbild Ihres Referenzcomputers fertigen Sie mit Windows PE und dem Tool ImageX an. Anschließend speichern Sie dieses Abbild in einer Netzwerkfreigabe. Auf einem Windows 7-Computer mit der Enterprise oder Ultimate Edition können Sie das Abbild statt-

dessen auch in einer VHD speichern und sie dann startfähig machen, wie in der Übung zu Lektion 2 weiter unten in diesem Kapitel beschrieben.

Gehen Sie folgendermaßen vor, um das Installationsabbild, das Sie auf Ihrem Referenzcomputer erstellt haben, in einer Netzwerkfreigabe aufzuzeichnen:

1. Legen Sie Ihr Windows PE-Medium in den Referenzcomputer ein und starten Sie den Computer neu. Wie schon erwähnt, müssen Sie unter Umständen die Startreihenfolge ändern, damit der Computer vom CD/DVD-Laufwerk startet. Drücken Sie in diesem Fall während des ersten Starts die entsprechende Funktionstaste, um die Startreihenfolge zu ändern.
2. Windows PE startet und öffnet ein Eingabeaufforderungsfenster. Zeichnen Sie mit dem Tool ImageX, das auf Ihrem Windows PE-Medium bereitliegt, ein Abbild Ihrer Referenzcomputerinstallation auf. Wenn beispielsweise *E:* Ihr optisches Laufwerk ist, *C:* die Installation enthält und Sie das aufgezeichnete Abbild auf Laufwerk *D:* speichern wollen, lautet der Befehl:

   ```
   e:\imagex.exe /capture c: d:\myimage.wim "Meine Win7-Installation" /compress fast
   /verify
   ```

3. Kopieren Sie das Abbild an einen Ort im Netzwerk. Dafür können Sie zum Beispiel folgende Befehle ausführen:

   ```
   net use y: \\network_share\images
   copy d:\myimage.wim y:
   ```

4. Geben Sie bei Bedarf die Anmeldeinformationen für den erforderlichen Netzwerkzugriff ein. Ihr Abbild liegt nun auf Volume *Y:* bereit.

Bereitstellen aus einer Netzwerkfreigabe

Sobald Sie ein Abbild Ihrer Referenzinstallation angefertigt haben, können Sie es auf einem oder mehreren Zielcomputern bereitstellen. Dieser Abschnitt beschreibt, wie Sie das von Hand durchführen. Kapitel 3 beschäftigt sich mit MDT 2010 und der automatischen Installation mehrerer Clientcomputer.

Wenn Sie ein Abbild aus einer Netzwerkfreigabe heraus bereitstellen, formatieren Sie zuerst das Festplattenlaufwerk eines Zielcomputers mit dem Tool Diskpart. Dann kopieren Sie das Abbild aus der Netzwerkfreigabe. Gehen Sie dazu folgendermaßen vor:

1. Legen Sie auf Ihrem Zielcomputer das Windows PE-Medium ein und starten Sie den Computer neu, indem Sie die Tastenkombination STRG+ALT+ENTF drücken. Windows PE öffnet ein Eingabeaufforderungsfenster.
2. Formatieren Sie das Festplattenlaufwerk so, dass es den Konfigurationsanforderungen entspricht. Rufen Sie dazu im Windows PE-Eingabeaufforderungsfenster das Tool Diskpart auf.
3. Geben Sie **diskpart** ein.
4. Geben Sie **select disk 0** ein.
5. Geben Sie **clean** ein.
6. Geben Sie **create partition primary size=100** ein.
7. Geben Sie **select partition 1** ein.
8. Geben Sie **format fs=ntfs label="System"** ein.

9. Geben Sie **assign letter=c** ein.
10. Geben Sie **active** ein.



Hinweis Systempartition

In den Schritten 6 bis 9 wird eine 100 MByte große Systempartition angelegt. Das ist nicht unbedingt nötig, weil die Windows 7-Installationsroutine bei der Installation automatisch eine Systempartition erstellt, sofern noch keine vorhanden ist. Microsoft empfiehlt aber, diese Partition vor der Installation anzulegen.

11. Geben Sie **create partition primary** ein.
12. Geben Sie **select partition 2** ein.
13. Geben Sie **format fs=ntfs label="Windows"** ein.
14. Geben Sie **assign letter=d** ein.
15. Geben Sie **exit** ein.



Hinweis Erstellen eines Skripts

Sie können ein Skript, das diese Informationen enthält, als Textdatei erstellen und am selben Speicherort wie Ihr Abbild ablegen. Geben Sie `diskpart /s <Skriptname>.txt` ein, um das Skript in einer Windows PE-Eingabeaufforderung auszuführen; dabei ist *<Skriptname>* der Name der Textdatei mit den Diskpart-Befehlen. Abbildung 2.8 zeigt eine typische Skriptdatei namens *DiskConfigurationFormat.txt*.

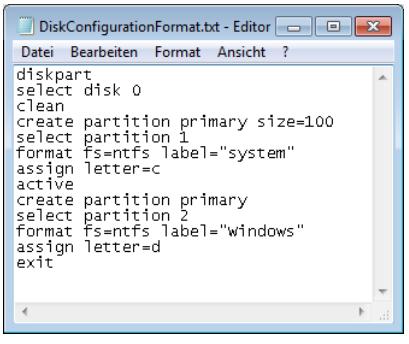


Abbildung 2.8 Eine Skriptdatei zum Formatieren der Festplatte

16. Kopieren Sie das Abbild aus der Netzwerkfreigabe auf Ihr lokales Festplattenlaufwerk. Führen Sie dazu in einer Eingabeaufforderung mit erhöhten Rechten beispielsweise folgende Befehle aus:

```
net use y: \\network_share\images
copy y:\myimage.wim d:
```

17. Geben Sie bei Bedarf die Anmeldeinformationen für den erforderlichen Netzwerkzugriff ein.

18. Wenden Sie das Abbild auf das Festplattenlaufwerk an. Dazu verwenden Sie das Tool ImageX, das auf dem Windows PE-Medium bereitliegt. Geben Sie in einer Eingabeaufforderung mit erhöhten Rechten ein:

    ```
    e:\imagex.exe /apply d:\myimage.wim 1 C:
    ```

19. Initialisieren Sie mit BCDboot den Startkonfigurationsdatenspeicher (Boot Configuration Data, BCD) und kopieren Sie die Startumgebungsdateien in die Systempartition. Geben Sie dazu in einer Eingabeaufforderung ein:

    ```
    d:\windows\system32\bcdboot d:\windows
    ```



Weitere Informationen BCDboot

Weitere Informationen über BCDboot finden Sie unter *http://technet.microsoft.com/de-de/library/cc721886.aspx*.

Ihr angepasstes Abbild ist nun auf dem Zielcomputer bereitgestellt. Der Computer kann somit an den Kunden ausgeliefert werden. Wiederholen Sie den Vorgang für jeden weiteren Computer, den Sie konfigurieren.



Weitere Informationen Windows 7-Bereitstellung

Weitere Informationen zum Installieren und Vorbereiten eines Referenzcomputers sowie zur Benutzung von Windows SIM, um Antwortdateien für eine automatische Installation zu erstellen, enthält *http://technet.microsoft.com/de-de/library/dd349348.aspx*.



Hinweis Architekturunabhängige Tools

Sowohl ImageX (x86) als auch Windows PE (x86) sind architekturübergreifende Tools. Sie können damit 32-Bit- und 64-Bit-Abbilder aufzeichnen.



Prüfungstipp

Machen Sie sich mit der Bedeutung von *Wimscript.ini*-, Festplattenkonfigurationsformat- und *Autounattend.xml*-Dateien vertraut. Lernen Sie, wie diese Dateien erstellt werden, wie darauf zugegriffen wird und wann sie eingesetzt werden.

Das WIM-Format

Mit dem Windows AIK-Tool ImageX können Sie eine WIM-Datei (Windows Imaging) erstellen, die das Abbild eines Referenzcomputers enthält. Im Unterschied zu ISO-Dateien, in denen Abbilder von Betriebssystemen und Toolkits im Intranet oder Internet verteilt werden, ist WIM ein dateibasiertes Datenträgerabbildformat, das einen ganzen Satz Dateien und die zugehörigen Dateisystemmetadaten enthält. Anders als sektorbasierte Formate (wie ISO), die für CD- und DVD-Abbilder benutzt werden, arbeitet WIM dateibasiert. Das bedeutet, dass eine Datei die kleinste Dateneinheit in einem WIM-Abbild ist. Ein dateibasiertes Abbild ist hardwareunabhängig, und es speichert immer nur ein einziges Exemplar einer Datei, selbst wenn sie mehrmals in der Dateisystemstruktur vorkommt.

Die Dateien sind innerhalb einer einzigen WIM-Datenbank gespeichert. Der Ressourcenaufwand zum Lesen oder Schreiben vieler Tausend einzelner Dateien auf einem lokalen Daten-

träger wird dadurch verringert, dass hardware- und softwarebasierte Zwischenspeicherung zum Einsatz kommen und Daten sequenziell gelesen und geschrieben werden. WIM-Abbilder werden auf einem vorhandenen Volume oder einer Partition bereitgestellt, weil die Tools keine Low-Level-Datenträgerstrukturen generieren und auch nicht formatieren. Stattdessen wird das Microsoft-Befehlszeilentool Diskpart eingesetzt, um Volumes auf dem Zielcomputer anzulegen und zu formatieren.

WIM-Dateien können mehrere Datenträgerabbilder enthalten, die entweder über einen numerischen Index oder einen eindeutigen Namen identifiziert werden. Weil WIM nur jeweils ein Exemplar einer Datei speichert, auch wenn sie mehrmals im Dateisystem verwendet wird, sind Daten, die in mehreren Abbildern benutzt werden, nur einmal gespeichert. Werden daher weitere Abbilder hinzugefügt, brauchen sie im Allgemeinen weniger Festplattenplatz als das erste. Eine WIM kann in mehrere Teile aufgeteilt werden, es handelt sich dann um ein sogenanntes übergreifendes Volume (spanned volume). Die Teile eines solchen übergreifenden WIM-Abbilds haben die Erweiterung *.swm*.

Ein WIM-Abbild kann auch als neues Volume unter Windows bereitgestellt werden, das einen Laufwerkbuchstaben zugeordnet bekommt, sodass sein Inhalt einfacher ausgelesen oder bearbeitet werden kann. Der Gerätetreiber *WimFltr.sys* muss geladen sein, bevor ein WIM-Abbild mit ImageX bereitgestellt wird.

Die DLL (Dynamic Link Library) *Wimgapi.dll* stellt einen Satz öffentlicher Programmierschnittstellen (Application Programming Interface, API) für die Bearbeitung von WIMs zur Verfügung. Auch etliche Anwendungen anderer Hersteller bieten die Möglichkeit, WIM-Dateien zu lesen und zu schreiben. Sie können WIM-Abbilder startfähig machen, indem Sie das Tool ImageX mit dem Argument `/boot` aufrufen.

Schnelltest

1. Welche Datei können Sie bei Bedarf erstellen, um das Tool ImageX anzuweisen, dass es die angegebenen Dateien und Ordner beim Aufzeichnen eines Systemabbilds ausschließt?
2. Wie findet ImageX diese Datei?

Antwort zum Schnelltest

1. Die Datei *Wimscript.ini*.
2. Speichern Sie die Datei im selben Ordner wie das Tool ImageX (*Imagex.exe*), dann erkennt ImageX sie automatisch.

Verteilen eines Abbilds auf viele Computer

Dieser Abschnitt beschreibt, wie Sie ein WIM-Abbild von einem Referenzcomputer aufzeichnen und es von Hand auf einen oder mehrere Zielcomputer verteilen. Haben Sie allerdings sehr viele Zielcomputer, ist die manuelle Verteilung mühsam und zeitaufwendig. Um das zu vermeiden, brauchen Sie eine automatisierte Methode, um ein Abbild gleichzeitig auf viele Computer in Ihrem Netzwerk zu verteilen.

Kapitel 1 stellte die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS) vor. Sie eignen sich für Zielcomputer, die über PXE starten. Wollen Sie dagegen mithilfe von WDS ein Abbild auf einen nicht PXE-fähigen Computer verteilen, müssen Sie diesen

Computer so starten, dass er ein WDS-Aufzeichnungsabbild ausführt. WDS-Abbilder werden weiter unten in dieser Lektion beschrieben.

Windows 7 führt MDT 2010 ein, ein leistungsfähiges Tool, mit dem Sie Systemabbilder auf mehrere Zielcomputer verteilen. Kapitel 3 beschreibt MDT 2010 genauer, hier beschränken wir uns daher auf einen groben Überblick.

Arbeiten mit MDT 2010

MDT 2010 ist die Microsoft-Lösung für die Bereitstellung von Betriebssystemen und Anwendungen. Es bietet flexible Treiberverwaltung, optimierte Transaktionsverarbeitung und Zugriff auf Bereitstellungsfreigaben von beliebigen Orten aus. Sie können MDT auf Abbilderstellungs- und Bereitstellungsservern einsetzen, um die automatische Bereitstellung von Windows 7 (oder anderen Betriebssystemen) auf Clientcomputern durchzuführen. Es ist möglich, MDT 2010 auf einem Windows 7-Client auszuführen, in der Praxis wird dafür allerdings meist ein Distributionsserver verwendet, der unter Windows Server 2008 läuft.

MDT stellt detaillierte Leitfäden und Auftragsplanungshilfen zur Verfügung. Seine zentrale Bereitstellungskonsole umfasst einheitliche Tools und Prozesse, die Sie für alle Client- und Serverbereitstellungen einsetzen können. Das Toolkit stellt standardisierte Desktop- und Serverabbilder zur Verfügung und verbessert die Sicherheit sowie die Konfigurationsverwaltung.

Mithilfe der LTI-Methode (Lite Touch Installation) können Sie Abbilder so verteilen, dass nur wenige Benutzereingaben erforderlich sind. Diese Methode kann eingesetzt werden, wenn keine anderen Verteilungstools vorhanden sind. Die meisten neuen Features in MDT 2010 betreffen LTI.

Die ZTI-Methode (Zero Touch Installation) kommt ganz ohne Benutzereingaben aus, allerdings muss dabei Microsoft System Center Configuration Manager (SCCM) 2007 mit dem Feature Pack *Operating System Deployment* im Netzwerk verfügbar sein. Diese Methode setzt zusätzlich einige weitere Programme voraus, zum Beispiel Microsoft SQL Server.



Hinweis System Management Server (SMS) 2003

MTD 2010 kann ZTI nicht mit SMS 2003 implementieren.

Wenn Sie MDT 2010 installiert haben, können Sie die Deployment Workbench aus der Programmfamilie des Microsoft Deployment Toolkits starten. Daraufhin haben Sie Zugriff auf folgende Elemente:

- **Informationscenter (Information Center)** Hier haben Sie Zugriff auf die MDT 2010-Dokumentation.
- **Bereitstellungsfreigabe (Deployment Share)** Hier führen Sie alle Aufgaben durch, die nötig sind, bevor Sie ein Betriebssystem bereitstellen. Sie können hier auch ein Bereitstellungsfreigabeverzeichnis erstellen.
- **Tasksequenzen (Task Sequences)** Enthält eine Detailansicht der Tasksequenzen. Sie können hier eine Tasksequenz zusammenstellen und konfigurieren.
- **Erweiterte Konfiguration (Advanced Configuration)** Wenn Sie dieses Element aufklappen, bekommen Sie die Bereitstellungspunkte und Datenbankelemente angezeigt, außerdem können Sie Bereitstellungsfreigaben und die MDT-Datenbank konfigurieren.



Weitere Informationen MDT 2010

Unter *http://technet.microsoft.com/en-us/solutionaccelerators/dd407791.aspx* können Sie die MDT-Dokumentationsdateien herunterladen, ohne dafür die Software installieren zu müssen.

WDS-Abbilder

WDS stellt eine über PXE gestartete Windows PE-Version zur Verfügung. Dabei wird ein WDS-Abbild in eine WIM-Datei verpackt und über das Netzwerk in einem RAM-Laufwerk gestartet. Anschließend wird die Installation unter Windows PE fortgesetzt.

WDS bietet die Möglichkeit zur Integration mit den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS), aber bei Bedarf kann der PXE-Server auch ohne AD DS laufen. WDS funktioniert auch mithilfe einer Windows PE-Version, die nicht über PXE gestartet wird, sondern beispielsweise von einer CD/DVD oder einem UFD.

Der Ablauf der Aufzeichnung eines WIM-Abbilds auf einem WDS-Server ähnelt dem Einsatz von ImageX und Sysprep, allerdings wird im letzten Schritt das WDS-Aufzeichnungsabbild gestartet. Dies ist ein Windows PE-Abbild, das Ihnen hilft, ein Clientsystem in einem WDS-Server aufzuzeichnen.

WDS ist deutlich schlanker als andere Methoden zur Abbildsbereitstellung, etwa MDT. Es ist außerdem oft schneller als die Windows-Installation von optischen Medien.

Sie verwenden WDS-Abbilder, um Systemdateien auf Clientcomputern bereitzustellen. Es gibt eine Reihe unterschiedlicher Abbilddateien. Beispielsweise verwenden Sie ein Aufzeichnungsabbild, um ein Installationsabbild zu erstellen. Sie sollten mit folgenden Abbildtypen vertraut sein:

- Installationsabbild (install image)
- Startabbild (boot image)
- Aufzeichnungsabbild (capture image)
- Suchabbild (discover image)

Ein Installationsabbild ist ein Betriebssystemabbild, das Sie auf dem Clientcomputer bereitstellen. Dies ist im Allgemeinen eine WIM-Datei.

Ein Startabbild ist ein Windows PE-Abbild, unter dem Sie einen Client starten, bevor Sie die WIM-Abbilddatei installieren. Um Windows 7 zu installieren, starten Sie den Computer erst unter dem Startabbild und wählen dann das Installationsabbild aus, das Sie installieren wollen. Sofern Sie keinen Referenzcomputer verwenden und keine Anwendungen zum Abbild hinzufügen, sollten Sie das Standardstartabbild nehmen, das auf dem Windows 7-Installationsmedium enthalten ist (*Install.wim*). Aufzeichnungs- und Suchabbilder sind spezielle Typen von Startabbildern.

Ein Aufzeichnungsabbild ist ein bestimmter Typ eines Startabbilds, unter dem Sie einen Clientcomputer starten, um das Betriebssystem in Form einer WIM-Installationsabbilddatei aufzuzeichnen. Sie erstellen ein Aufzeichnungsabbild, bevor Sie ein benutzerdefiniertes Installationsabbild anfertigen. Ein Aufzeichnungsabbild enthält Windows PE und den Assistenten zur Abbildaufzeichnung aus den Windows-Bereitstellungsdiensten. Wenn Sie einen Computer (nachdem Sie ihn mit Sysprep vorbereitet haben) unter einem Aufzeichnungsabbild starten, erstellt der Assistent ein Installationsabbild des Computers und speichert es als

WIM-Datei. Anschließend können Sie das Abbild auf den WDS-Server hochladen oder es auf ein startfähiges Medium (zum Beispiel eine DVD) kopieren.

Ein Suchabbild ist ein Typ eines Startabbilds, das Sie einsetzen, um Windows 7 (oder andere Windows-Betriebssysteme) auf einem Computer zu installieren, der nicht PXE-fähig ist. Wenn Sie einen Computer unter einem Suchabbild starten, sucht der WDS-Client nach einem gültigen WDS-Server und lässt Sie auswählen, welches Installationsabbild Sie installieren wollen. Mithilfe eines Suchabbilds ist ein Computer in der Lage, einen WDS-Server zu finden und ein Abbild davon zu installieren.



Weitere Informationen Erstellen von Abbildern

Weitere Informationen darüber, wie Sie Abbilder erstellen, finden Sie unter *http://technet.microsoft.com/de-de/library/cc730907.aspx*. Diese Seiten behandeln Windows Server 2008, weil WDS eine Serverrolle ist, die nicht auf einem Clientcomputer installiert werden kann.

Verwenden von DISM

Windows 7 führt das neue Befehlszeilentool DISM ein (Deployment Image Servicing and Management Tool, Tool zur Abbildverwaltung für die Bereitstellung). Kapitel 3 beschreibt dieses Tool genauer, daher beschränken wir uns hier auf einen kurzen Überblick. Sie verwenden DISM, um ein Windows-Abbild zu bearbeiten oder ein Windows PE-Abbild vorzubereiten. DISM ersetzt die Programme Packet Manager (*Pkgmgr.exe*), PEimg und Intlcfg aus Windows Vista und führt neue Features ein, die es einfacher machen, Offlineabbilder zu bearbeiten.

Sie können in DISM folgende Aufgaben durchführen:

- Vorbereiten eines Windows PE-Abbilds
- Aktivieren oder Deaktivieren von Windows-Features innerhalb eines Abbilds
- Durchführen eines Upgrades eines Windows-Abbilds auf eine andere Edition
- Hinzufügen, Entfernen und Auflisten von Paketen
- Hinzufügen, Entfernen und Auflisten von Treibern
- Anwenden von Änderungen anhand des Abschnitts für die Offlinebearbeitung in einer Antwortdatei
- Konfigurieren internationaler Einstellungen
- Implementieren leistungsfähiger Protokollierungsfeatures
- Pflegen von Betriebssystemen wie Windows Vista mit SP1 und Windows Server 2008
- Bearbeiten eines 32-Bit-Abbilds auf einem 64-Bit-Host oder eines 64-Bit-Abbilds auf einem 32-Bit-Host
- Bearbeiten aller Plattformen (32 Bit, 64 Bit und Itanium)
- Benutzen vorhandener Paketmanagerskripts

Befehlszeilenoptionen von DISM

Damit Sie ein Windows-Abbild offline bearbeiten können, müssen Sie es anwenden oder im Dateisystem bereitstellen (mount). WIM-Abbilder können mit den WIM-Befehlen von DISM bereitgestellt oder angewendet werden; sobald Sie mit dem Bearbeiten fertig sind, zeichnen Sie das Abbild mit ImageX neu auf. Sie können die WIM-Befehle auch verwenden, um die

Indizes aufzulisten oder die Architektur des Abbilds zu überprüfen, das Sie im Dateisystem bereitstellen. Sobald Sie das Abbild verändert haben, müssen Sie seine Bereitstellung im Dateisystem aufheben (unmount) und dann die vorgenommenen Änderungen entweder übernehmen (commit) oder verwerfen (discard).

Tabelle 2.4 beschreibt die Befehlszeilenoptionen von DISM, mit denen Sie WIM-Dateien im Dateisystem bereitstellen, ihre Bereitstellung im Dateisystem aufheben und WIM-Dateien abfragen. Die Tabelle listet auch die zugehörigen Flags auf. Bei diesen Optionen und Flags wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Tabelle 2.4 Befehlszeilenoptionen von DISM

Option	Beschreibung	Flags
`/mount-wim`	Stellt die WIM-Datei im angegebenen Verzeichnis des Dateisystems bereit, sodass sie bearbeitet werden kann. Das optionale Flag `/readonly` bindet das bereitgestellte Abbild schreibgeschützt ein. Beispiel: `dism /mount-wim /wimfile:C:\practice\myimages\install.wim /index:1 /mountdir:C:\practice\offline /readonly`	`/wimfile:`*`<Pfad_zur_image.wim>`* `/index:`*`<Abbildindex>`* `/name:`*`<Abbildname>`* `/mountdir:`*`<Pfad_zum_Bereitstellungsverzeichnis>`* `/readonly`
`/commit-wim`	Wendet die Änderungen an, die Sie am bereitgestellten Abbild vorgenommen haben. Das Abbild bleibt bereitgestellt, bis die Option `/dismount` verwendet wird. Beispiel: `dism /commit-wim /mountdir:C:\practice\offline`	`/mountdir:`*`<Pfad_zum_Bereitstellungsverzeichnis>`*
`/unmount-wim`	Hebt die Bereitstellung der WIM-Datei im Dateisystem auf und übernimmt oder verwirft die Änderungen, die durchgeführt wurden, während das Abbild bereitgestellt war. Beispiel: `dism /unmount-wim /mountdir:C:\practice\offline /commit`	`/mountdir:`*`<Pfad_zum_Bereitstellungsverzeichnis>`*`{/commit | /discard}`
`/remount-wim`	Stellt ein verwaistes WIM-Bereitstellungsverzeichnis wieder her. Beispiel: `dism /remount-wim /mountdir:`*`<Pfad_zum_Bereitstellungsverzeichnis>`*	`/mountdir:`*`<Pfad_zum_Bereitstellungsverzeichnis>`*
`/cleanup-wim`	Löscht alle Ressourcen, die mit einem bereitgestellten WIM-Abbild verknüpft sind, das aufgegeben wurde. Dieser Befehl hebt nicht die Bereitstellung momentan eingebundener Abbilder auf und löscht auch keine Abbilder, die erneut im Dateisystem bereitgestellt werden können. Beispiel: `dism /cleanup-wim`	Keine

▶

Option	Beschreibung	Flags

`/get-wiminfo`	Zeigt Informationen über die Abbilder innerhalb der WIM an. Wird zusätzlich `/index` verwendet, werden Informationen über das angegebene Abbild angezeigt.
	Beispiel: `dism /get-wimInfo /wimfile: C:\practice\offline\install.wim /index:1`
		`/wimfile:<Pfad_zur_image.wim>`
		`/index:<Abbildindex>`
		`/name:<Abbildname>`

`/get-mountedwiminfo`	Listet die Abbilder auf, die momentan bereitgestellt sind, und zeigt Informationen über jedes bereitgestellte Abbild an, darunter Lese-/Schreibberechtigungen, Bereitstellungsverzeichnis, Pfad der bereitgestellten Datei und Index des bereitgestellten Abbilds.
	Beispiel: `dism /get-mountedwiminfo`
		`/name:<Abbildname>`
		`/mountdir:<Pfad_zum_Bereitstellungsverzeichnis>`
		`/readonly`

Syntax von DISM

DISM-Befehle haben eine Grundsyntax, die bei allen Befehlen recht ähnlich ist. Sobald Sie Ihr Windows-Abbild im Dateisystem bereitgestellt haben, können Sie DISM-Optionen, den Bearbeitungsbefehl zum Verändern Ihres Abbilds und den Speicherort des bereitgestellten Abbilds angeben. Sie dürfen pro Befehlszeile nur einen einzigen Bearbeitungsbefehl verwenden. Sofern Sie einen laufenden Computer bearbeiten, können Sie die Option `/online` verwenden, statt den Speicherort des bereitgestellten Windows-Abbilds anzugeben.

Die Syntax für DISM lautet:

`DISM.exe {/image:<Pfad_zum_Abbild> | /online} [DISM-Optionen] {Bearbeitungsbefehl} [<Bearbeitungsargument>]`



Prüfungstipp

Sie verwenden DISM, um vorhandene Abbilder zu bearbeiten, aber Sie können mit diesem Tool keine neuen Betriebssystemabbilder aufzeichnen.

Vorbereiten einer Windows 7-Installation mit Sysprep

Mit dem Befehlszeilentool Sysprep (Systemvorbereitungsprogramm) bereiten Sie eine Windows-Installation auf die Abbilderstellung oder die Auslieferung an einen Benutzer vor. Die Befehle `sysprep /generalize` und `sysprep /oobe` wurden bereits weiter oben in dieser Lektion erwähnt. Sysprep ist ein leistungsfähiges Tool, die ausführbare Datei (*Sysprep.exe*) liegt im Verzeichnis *%WinDir%\System32\Sysprep*. Nach dem Start prüft *Sysprep.exe* zuerst, ob Sysprep ausgeführt werden kann. Sie können Sysprep nur als Administrator ausführen, und es darf immer nur eine einzige Instanz von Sysprep laufen. Zu jeder Windows-Version gibt es eine andere Version von Sysprep. Sysprep muss unter der Windows-Version laufen, in der es installiert wurde.

Sysprep.exe ruft andere ausführbare Dateien auf, die die Windows-Installation vorbereiten. Der Sysprep-Prozess initialisiert die Protokollierung und wertet alle übergebenen Befehlszeilenparameter aus. Wurden keine Befehlszeilenparameter angegeben, öffnet sich das Sysprep-Fenster. Hier können Sie die gewünschten Aktionen auswählen. Sysprep führt diese

Aktionen aus und ruft die entsprechenden DLLs und ausführbaren Dateien auf. Dann fügt es die Aktionen zur Protokolldatei hinzu.

Sobald alle Aufgaben abgearbeitet sind, fährt Sysprep das System herunter und startet es neu, oder es beendet sich selbst.

Befehlszeilenoptionen von Sysprep

Falls Sie bereits Erfahrung mit Windows Vista haben, werden Ihnen die Befehlszeilenoptionen der Sysprep-Version in Windows 7 vertraut vorkommen. Tabelle 2.5 beschreibt die Befehlszeilenoptionen.

Tabelle 2.5 Befehlszeilenoptionen von Sysprep

Option	Beschreibung
`/audit`	Startet den Computer im Überwachungsmodus neu statt mit der Windows-Willkommensseite. Im Überwachungsmodus können Sie zusätzliche Treiber oder Anwendungen zu Windows 7 hinzufügen. Sie können auch eine Installation von Windows 7 testen und ihre Integrität prüfen, bevor sie an einen Benutzer gesendet wird. Wenn Sie eine Datei für das unbeaufsichtigte Windows-Setup angeben, führt der Windows-Setupmodus `/audit` die Konfigurationsdurchläufe *auditSystem* und *auditUser* aus.
`/generalize`	Bereitet die Windows-Installation vor, von der ein Abbild aufgezeichnet werden soll. Wenn Sie diese Option angeben, werden alle eindeutigen Systeminformationen aus der Windows-Installation gelöscht. Die SID wird zurückgesetzt, die Systemwiederherstellungspunkte werden gelöscht und die Ereignisprotokolle werden entfernt. Sobald der Computer das nächste Mal startet, wird der Konfigurationsdurchlauf *specialize* ausgeführt. Dabei wird eine neue SID erstellt und die Frist für die Windows-Aktivierung zurückgesetzt (sofern sie nicht schon dreimal zurückgesetzt wurde).
`/oobe`	Startet den Computer mit der Windows-Willkommensseite neu. Auf der Windows-Willkommensseite können Benutzer ihr Windows 7 anpassen, Benutzerkonten anlegen und den Namen des Computers festlegen. Alle Einstellungen aus dem *oobeSystem*-Konfigurationsdurchlauf in einer Antwortdatei werden verarbeitet, noch bevor die Windows-Willkommensseite startet.
`/reboot`	Startet den Computer neu. Sie können diese Option verwenden, um den Computer zu überwachen und zu überprüfen, ob der Ablauf beim ersten Einschalten wie gewünscht aussieht.
`/shutdown`	Fährt den Computer herunter, sobald Sysprep beendet ist.
`/quiet`	Führt Sysprep aus, ohne Bestätigungsmeldungen auf dem Bildschirm anzuzeigen. Mithilfe dieser Option können Sie Sysprep automatisieren.
`/quit`	Schließt Sysprep, sobald die angegebenen Befehle abgeschlossen sind.
`/unattend:` *<Antwortdatei>*	Wendet die Einstellungen aus einer Antwortdatei auf Windows an, während eine unbeaufsichtigte Installation läuft. Der Parameter *<Antwortdatei>* gibt den Pfad und den Dateinamen der Antwortdatei an.

Sofern Sie keine Befehlszeilenoption angeben, öffnet Sysprep eine grafische Benutzeroberfläche (Graphical User Interface, GUI), die Sie in Abbildung 2.9 sehen. Hier können Sie eine Systembereinigungsaktion festlegen, das Kontrollkästchen *Verallgemeinern* aktivieren und eine Option für das Herunterfahren auswählen.

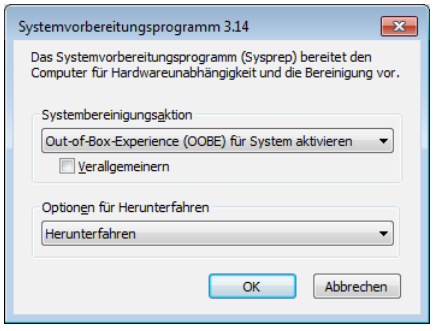


Abbildung 2.9 Die Benutzeroberfläche von Sysprep



Weitere Informationen Überwachungsmodus

Weitere Informationen zum Überwachungsmodus finden Sie unter *http://technet.microsoft.com/de-de/library/cc722413.aspx*.

Wenn Sie ein Windows 7-Abbild auf einen anderen Computer übertragen wollen, müssen Sie `sysprep /generalize` sogar dann ausführen, wenn der Zielcomputer dieselbe Hardwarekonfiguration hat. Der Befehl `sysprep /generalize` entfernt eindeutige Informationen aus Ihrer Windows 7-Installation. Auf diese Weise können Sie Ihr Abbild auf anderen Computern wiederverwenden. Sobald Sie das Windows 7-Abbild das nächste Mal starten, läuft der Konfigurationsdurchlauf *specialize*. Während dieses Durchlaufs werden viele Featureaktionen automatisch verarbeitet, sobald Sie ein Windows 7-Abbild auf einem neuen Computer starten. Alle Methoden, um ein Windows 7-Abbild auf einen neuen Computer zu kopieren, sei es mithilfe der Abbilderstellung oder durch Kopieren der Festplatte, müssen mit dem Befehl `sysprep /generalize` vorbereitet werden. Sie können ein Windows 7-Abbild nicht eher auf einen anderen Computer verschieben oder kopieren, als Sie `sysprep /generalize` ausgeführt haben.

Konfigurationsdurchläufe

Konfigurationsdurchläufe sind Phasen von Windows-Setup, in denen im Rahmen einer unbeaufsichtigten Installation die Einstellungen aus einer Antwortdatei angewendet werden. Tabelle 2.6 beschreibt die unterschiedlichen Konfigurationsdurchläufe.



Prüfungstipp

Machen Sie sich mit den Befehlszeilenoptionen von Sysprep sowie den Konfigurationsdurchläufen des Windows-Setups vertraut und prägen Sie sich ein, wann die Konfigurationsdurchläufe ausgeführt werden. Zum Beispiel läuft *generalize*, wenn Sie den Befehl `sysprep /generalize` ausführen, und *auditUser* sowie *auditSystem* laufen, wenn Sie im Überwachungsmodus starten. Denken Sie daran, dass Sie mehrere Sysprep-Optionen im selben Befehl angeben können. Beispielsweise können Sie ein Abbild verallgemeinern und den Systemstartmodus auswählen, indem Sie den Befehl **C:\Windows\system32\sysprep\Sysprep.exe /oobe /generalize /shutdown** ausführen. Lernen Sie auch, wie Sie den Computer im Überwachungsmodus starten (STRG+UMSCHALT+F3); dies wird weiter unten in dieser Lektion beschrieben.

Tabelle 2.6 Konfigurationsdurchläufe

Konfigurations-durchlauf	Beschreibung
windowsPE	Konfiguriert Windows PE-Optionen und grundlegende Windows-Setupoptionen. Diese Optionen legen beispielsweise den Product Key fest und konfigurieren ein Laufwerk. Sie können diesen Konfigurationsdurchlauf nutzen, um Treiber zum Windows PE-Treiberspeicher hinzuzufügen, und Treiber, die von Windows PE für den Startvorgang gebraucht werden, bereitzustellen, wenn sie nötig sind, damit Windows PE auf das lokale Festplattenlaufwerk oder ein Netzwerk zugreifen kann.
offlineServicing	Wendet Updates auf ein Windows-Abbild an. Wendet außerdem Pakete an, beispielsweise Softwarefixes, Language Packs und andere Sicherheitsupdates. Während dieses Durchlaufs können Sie Treiber zu einem Windows-Abbild hinzufügen, bevor es im Rahmen des Windows-Setups installiert wird.
specialize	Erstellt systemspezifische Informationen und wendet sie an. Zum Beispiel können Sie Netzwerkeinstellungen, internationale Einstellungen und Domäneninformationen konfigurieren.
generalize	Ermöglicht Ihnen, den Befehl `sysprep /generalize` und andere Windows-Einstellungen, die in Ihrem Referenzabbild erhalten bleiben müssen, in engen Grenzen zu konfigurieren. Der Befehl `sysprep /generalize` entfernt systemspezifische Informationen aus dem Abbild, darunter die eindeutige SID und andere hardwarespezifische Einstellungen. Der Durchlauf *generalize* wird nur ausgeführt, wenn Sie den Befehl `sysprep /generalize` ausführen.
auditSystem	Verarbeitet Einstellungen für das unbeaufsichtigte Setup, während Windows im Systemkontext läuft, bevor sich im Überwachungsmodus ein Benutzer am Computer anmeldet. Der Durchlauf *auditSystem* wird nur ausgeführt, wenn Sie im Überwachungsmodus starten.
auditUser	Verarbeitet Einstellungen für das unbeaufsichtigte Setup, nachdem sich im Überwachungsmodus ein Benutzer am Computer angemeldet hat. Der Durchlauf *auditUser* wird nur ausgeführt, wenn Sie im Überwachungsmodus starten.
oobeSystem	Wendet Einstellungen auf Windows an, bevor die Windows-Willkommensseite startet.

Antwortdateien für Sysprep

Mithilfe einer Sysprep-Antwortdatei können Sie Einstellungen für das unbeaufsichtigte Setup konfigurieren. Nicht alle Konfigurationsdurchläufe werden während des Windows-Setups ausgeführt. Einige stehen nur zur Verfügung, wenn Sie *Sysprep.exe* ausführen. Zum Beispiel stehen die Durchläufe *generalize*, *auditSystem* und *auditUser* nur zur Verfügung, wenn Sie *Sysprep.exe* ausführen. Wenn Sie Einstellungen zu diesen Konfigurationsdurchläufen in Ihre Antwortdatei einfügen, müssen Sie *Sysprep.exe* ausführen, um die Einstellungen anzuwenden.

Einstellungen für die Durchläufe *auditSystem* und *auditUser* wenden Sie an, indem Sie den Befehl `sysprep /audit` ausführen und so im Überwachungsmodus starten. Und Einstellungen für den Durchlauf *generalize* wenden Sie an, indem Sie das Windows-Abbild mit `sysprep /generalize` verallgemeinern.

Wenn Sie Windows mithilfe einer Antwortdatei (etwa *Autounattend.xml*) installieren, wird sie zwischengespeichert. Laufen spätere Konfigurationsdurchläufe, werden die Einstellun-

gen aus der Antwortdatei auf das System angewendet. Weil die Antwortdatei zwischengespeichert wird, werden die Einstellungen aus der zwischengespeicherten Antwortdatei angewendet, wenn Sie *Sysprep.exe* ausführen. Wollen Sie die Einstellungen aus einer anderen Antwortdatei verwenden, können Sie mit der Option `sysprep /unattend:<Dateiname>` eine separate Antwortdatei angeben. In diesem Fall muss die Antwortdatei eine *.xml*-Datei sein, die aber nicht *Autounattend.xml* heißt.

Im Fensterabschnitt *Antwortdatei* von Windows SIM können Sie diese Datei erstellen. Für ihre Bearbeitung können Sie auch einen beliebigen Texteditor wie beispielsweise den Windows-Editor (Notepad) verwenden. Manche erfahrene Administratoren erstellen Antwortdateien lieber mit einem Texteditor als mit Windows SIM.



Weitere Informationen Erstellen einer Antwortdatei mit Windows SIM

Eine Schritt-für-Schritt-Anleitung, wie Sie Antwortdateien für die unbeaufsichtigte Installation erstellen, finden Sie unter *http://technet.microsoft.com/de-de/library/dd349348.aspx*.



Hinweis Behalten von Plug & Play-Gerätetreibern während des Durchlaufs *generalize*

Sie können Gerätetreiber behalten, wenn Sie den Befehl `sysprep /generalize` ausführen. Verändern Sie dazu die Einstellung `PersistentAllDeviceInstalls` im Feature *Microsoft-Windows-PnPSysprep*. Während des Durchlaufs *specialize* durchsucht Plug & Play den Computer nach Geräten und installiert Gerätetreiber für alle gefundenen Geräte. In der Standardeinstellung werden diese Gerätetreiber aber wieder aus dem System gelöscht, wenn Sie das System verallgemeinern. Wenn Sie `PersistAllDeviceInstalls` in einer Antwortdatei auf den Wert `true` setzen, entfernt Sysprep die erkannten Gerätetreiber nicht.

Sie können sich den Status der `RunSynchronous`-Befehle ansehen, die während des Durchlaufs *auditUser* im Überwachungsmodus ausgeführt werden. Das Fenster *AuditUI* führt den Status der Befehle auf und zeigt den Fortschritt grafisch an. So erkennen Sie, ob die Installation noch läuft oder angehalten wurde. Außerdem sehen Sie, wann und wo Fehler auftreten.

Gibt es `RunSynchronous`-Befehle in der Antwortdatei, die während des Konfigurationsdurchlaufs *auditUser* ausgeführt werden, wird eine Liste der Befehle im Fenster *AuditUI* in der Reihenfolge angezeigt, die in `RunSynchronous/RunSynchronousCommand/Order` festgelegt ist.

Alle `RunSynchronous`-Befehle werden in der angegebenen Reihenfolge verarbeitet. War ein Befehl erfolgreich, wird das zugehörige Listenelement mit einem grünen Häkchen markiert. Tritt bei der Ausführung des Befehls dagegen ein Fehler auf, wird das entsprechende Listenelement mit einem rotem Kreuz hervorgehoben. Wird ein Neustart angefordert, wird nach dem Neustart erneut *AuditUI* angezeigt, aber diesmal werden nur Listenelemente aufgeführt, die noch nicht verarbeitet wurden.

Enthält die Liste in *AuditUI* mehr Elemente, als in das Fenster passen, wird die Liste abgeschnitten, sie wird nicht umgeblättert. In diesem Fall sind daher einige Elemente nicht sichtbar.

Zurücksetzen der Windows 7-Aktivierung

Wenn Sie Windows 7 mit einem einzelnen Product Key installieren, haben Sie 30 Tage Zeit, um diese Windows-Installation zu aktivieren. Versäumen Sie es, Windows während dieser 30-Tage-Frist zu aktivieren, schaltet es in den Modus mit verringertem Funktionsumfang

(Reduced Functionality Mode, RFM). Sie können sich dann erst wieder am Computer anmelden, wenn Windows 7 aktiviert ist.

Wenn Sie den Befehl `sysprep /generalize` ausführen, wird der Aktivierungszähler automatisch zurückgesetzt. Sie können Windows mit `sysprep /generalize` aber höchstens dreimal zurücksetzen. Nachdem Sie `sysprep /generalize` zum dritten Mal ausgeführt haben, ist es nicht mehr möglich, den Aktivierungszähler zurückzusetzen.

Sie können verhindern, dass der Aktivierungszähler zurückgesetzt wird, wenn Sie die Einstellung `SkipRearm` im Feature *Microsoft-Windows-Security-Licensing-SLC* konfigurieren. Wenn Sie `SkipRearm` im Befehl `sysprep /generalize` auf den Wert 1 setzen, wird der Aktivierungszähler beim Ausführen von Sysprep nicht zurückgesetzt.



Weitere Informationen Microsoft-Windows-Security-Licensing-SLC

Weitere Informationen über das Feature *Microsoft-Windows-Security-Licensing-SLC* finden Sie unter *http://technet.microsoft.com/en-us/library/cc766403.aspx*. Diese Seite behandelt Windows Vista, die Informationen gelten aber genauso für Windows 7.

Bei Volumenlizenzen unterscheidet sich das Verhalten beim Zurücksetzen des Aktivierungszählers abhängig vom Typ der Lizenz. Bei aktivierten Schlüsselverwaltungsdienstclients (Key Management Service, KMS) kann der Aktivierungszähler beliebig oft zurückgesetzt werden. Dagegen kann der Aktivierungszähler bei nicht aktivierten KMS-Clients höchstens dreimal zurückgesetzt werden, genauso wie bei Einzellizenzen.

Microsoft empfiehlt, für KMS-Clients den Befehl `sysprep /generalize` so auszuführen, dass die Einstellung `SkipRearm` den Wert 1 hat. Sobald das Abbild aufgezeichnet ist, sollten Sie den Befehl `sysprep /generalize` erneut ausführen, wobei `SkipRearm` den Wert 0 hat.

Microsoft empfiehlt, für MAK-Clients (Multiple Activation Keys) den MAK sofort zu installieren, sobald Sysprep zum letzten Mal ausgeführt wurde, bevor ein Clientcomputer an einen Benutzer ausgeliefert wird.

Bei OEM-Aktivierungslizenzen ist im Allgemeinen keine Aktivierung erforderlich. Die OEM-Aktivierung steht nur für Royalty-OEMs zur Verfügung.

Die meisten Benutzer können die Aktivierung erledigen, nachdem sie ihren Windows 7-Client erhalten haben. Wenn es Ihnen lieber ist, können Sie die Software allerdings auch für Ihre Benutzer aktivieren. Nachdem die Aktivierung erledigt ist, brauchen die meisten Benutzer ihre Installation nicht noch einmal zu aktivieren.

Um Windows auf einem Clientcomputer zu aktivieren, brauchen Sie den eindeutigen Product Key, der auf dem »Certificate of Authenticity«-Aufkleber (COA) aufgedruckt ist. Diesen Aufkleber finden Sie gewöhnlich auf dem Computergehäuse. Führen Sie den Befehl `sysprep /oobe` aus, um den Computer für die Auslieferung an den Benutzer vorzubereiten.

Starten im Überwachungsmodus oder mit der Windows-Willkommensseite

Wenn Windows 7 startet, schaltet der Computer in einen der folgenden Modi:

- **Windows-Willkommensseite** In der Standardeinstellung starten alle Windows-Installationen zuerst die Windows-Willkommensseite. Die Windows-Willkommensseite (Windows Welcome) wird auch als »Machine OOBE« bezeichnet, deshalb heißt der entsprechende Konfigurationsdurchlauf *oobeSystem*. Hier kommt der Benutzer zum ersten Mal mit seinem neuen Windows 7-System in Berührung und kann die Windows-

Installation nach seinen Vorlieben anpassen. Die Benutzer können Benutzerkonten anlegen, die Microsoft-Softwarelizenzbedingungen lesen und annehmen sowie Sprache und Zeitzone auswählen. Der Konfigurationsdurchlauf *oobeSystem* wird sofort ausgeführt, noch bevor die Windows-Willkommensseite startet.

- **Überwachungsmodus** Im Überwachungsmodus können große Organisationen ihre Windows-Abbilder anpassen. Die Konfigurationseinstellungen aus der Windows-Willkommensseite brauchen im Überwachungsmodus nicht angewendet zu werden. Indem Sie die Windows-Willkommensseite überspringen, können Sie schneller auf den Desktop zugreifen, um die erforderlichen Anpassungen vorzunehmen. Sie können beispielsweise weitere Gerätetreiber hinzufügen, Anwendungen installieren und die Installation überprüfen. Im Überwachungsmodus werden die Einstellungen für die Konfigurationsdurchläufe *auditSystem* und *auditUser* aus einer Antwortdatei für die unbeaufsichtigte Installation verarbeitet.

Wenn der Computer im Überwachungsmodus läuft, können Sie den Befehl `sysprep /oobe` ausführen, um die Installation so zu konfigurieren, dass sie mit der Windows-Willkommensseite startet. In der Standardeinstellung wird die normale Windows-Willkommensseite geöffnet, sobald die Installation abgeschlossen ist. Sie können die Windows-Willkommensseite allerdings überspringen und direkt im Überwachungsmodus starten, indem Sie beim Erscheinen der Windows-Willkommensseite die Tastenkombination STRG+UMSCHALT+F3 drücken.

Bei einer unbeaufsichtigten Installation können Sie Windows mithilfe der Einstellung `Microsoft-Windows-Deployment/Reseal` in einer Antwortdatei so konfigurieren, dass es im Überwachungsmodus startet.



Weitere Informationen Überwachungsmodus

Weitere Informationen über den Überwachungsmodus enthält *http://technet.microsoft.com/de-de/library/cc722413.aspx*. Diese Seite behandelt Windows Vista, die Informationen gelten aber genauso für Windows 7.



Weitere Informationen Ermitteln des Status eines Windows-Abbilds

Sie können feststellen, in welchem Status sich ein Windows-Abbild befindet, ob es beispielsweise im Überwachungsmodus oder mit der Windows-Willkommensseite startet oder ob das Abbild noch in der Installationsphase ist. Weitere Informationen finden Sie unter *http://technet.microsoft.com/de-de/library/cc721913.aspx*. Diese Seite behandelt Windows Vista, die Informationen gelten aber genauso für Windows 7.

Sysprep-Protokolldateien

Sysprep protokolliert die Windows-Setupaktionen in unterschiedlichen Verzeichnissen, die vom Konfigurationsdurchlauf abhängen. Weil der Durchlauf *generalize* einige Windows-Setupprotokolldateien löscht, zeichnet Sysprep *generalize*-Aktionen außerhalb der üblichen Windows-Setupprotokolldateien auf. Tabelle 2.7 zeigt, wo die von Sysprep benutzten Protokolldateien liegen.

Tabelle 2.7 Speicherorte der Sysprep-Protokolldateien

Element	Pfad der Protokolldatei
Durchlauf *generalize*	*%WinDir%\System32\Sysprep\Panther*
Durchlauf *specialize*	*%WinDir%\Panther*
Aktionen beim unbeaufsichtigten Windows-Setup	*%WinDir%\Panther\Unattendgc*

Übung Erstellen eines WIM-Abbilds

In dieser Übung installieren Sie das Windows AIK. Anschließend erstellen Sie einen Windows PE-Startdatenträger und starten den Computer mit Windows PE. Auf diese Weise können Sie mit dem Tool ImageX aus dem Windows AIK ein WIM-Abbild des Computers anlegen.

Übung 1 Installieren des Windows AIK und Erstellen einer Windows PE-Start-DVD

In dieser Übung laden Sie das ISO-Abbild des Windows AIK herunter und erstellen eine Installations-DVD. Dann installieren Sie das Windows AIK. Wie Sie dabei vorgehen, wurde im Abschnitt »Installieren und Benutzen des Windows Automated Installation Toolkit« weiter oben in dieser Lektion beschrieben. Sie legen ein Windows PE-Buildverzeichnis an und kopieren ImageX hinein. Mit dem Tool Oscdimg erstellen Sie ein ISO-Abbild von Windows PE. Dieses Abbild brennen Sie auf einen CD- oder DVD-Rohling, von dem Sie den Computer anschließend starten. Sie brauchen eine Internetverbindung, um diese Übung durcharbeiten zu können.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Laden Sie das passende ISO-Abbild herunter, brennen Sie es auf DVD und installieren Sie das Windows AIK.
3. Klicken Sie unter *Alle Programme/Zubehör* mit der rechten Maustaste auf *Eingabeaufforderung* und wählen Sie den Befehl *Als Administrator ausführen*. Klicken Sie auf *Ja*, falls Sie gefragt werden, ob Sie die Ausführung des Programms genehmigen.
4. Geben Sie im Eingabeaufforderungsfenster **cd C:\Program Files\Windows AIK\Tools\PETools** ein.
5. Geben Sie in der Eingabeaufforderung *C:\Program Files\Windows AIK\Tools\PETools>* den Befehl **copype.cmd x86 c:\winpe_x86** ein. Diese Übung ist für einen 32-Bit-Computer geschrieben, das Windows PE-Buildverzeichnis ist in diesem *Winpe_x86*. Verwenden Sie stattdessen einen AMD64 oder IA64-Computer, müssen Sie das Verzeichnis entsprechend anpassen. Abbildung 2.10 zeigt die Ausgabe dieses Befehls.
6. Führen Sie den Befehl **copy c:\winpe_x86\winpe.wim c:\winpe_x86\ISO\Sources\boot.wim** aus, um die erforderliche WIM-Datei in das Windows PE-Buildverzeichnis zu kopieren.
7. Kopieren Sie ImageX in das Windows PE-Buildverzeichnis, indem Sie den Befehl **copy "c:\Program Files\Windows AIK\Tools\x86\imagex.exe" c:\winpe_x86\iso** ausführen.
8. Erstellen Sie mit dem Tool Oscdimg eine Abbilddatei (*.iso*), indem Sie auf *Alle Programme*, dann auf *Microsoft Windows AIK* und schließlich auf *Eingabeaufforderung für Bereitstellungstools* klicken.

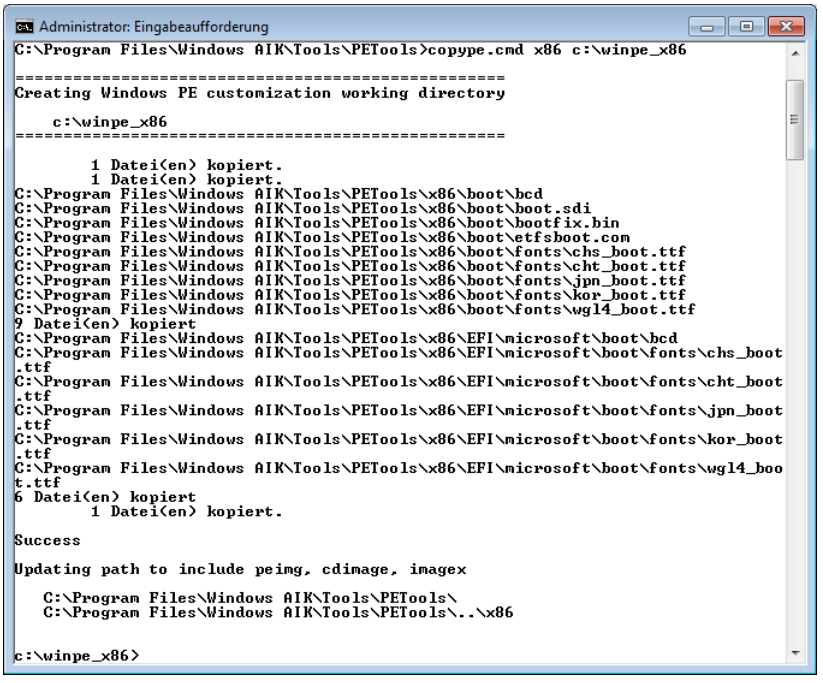


Abbildung 2.10 Erstellen des Windows PE-Buildverzeichnisses

9. Geben Sie den Befehl **oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso** ein, um das ISO-Abbild zu erstellen. Abbildung 2.11 zeigt die Ausgabe dieses Befehls. Beachten Sie, dass kein Leerzeichen zwischen dem Argument `-b` und dem Pfad *c:\winpe_x86\etfsboot.com* stehen darf.

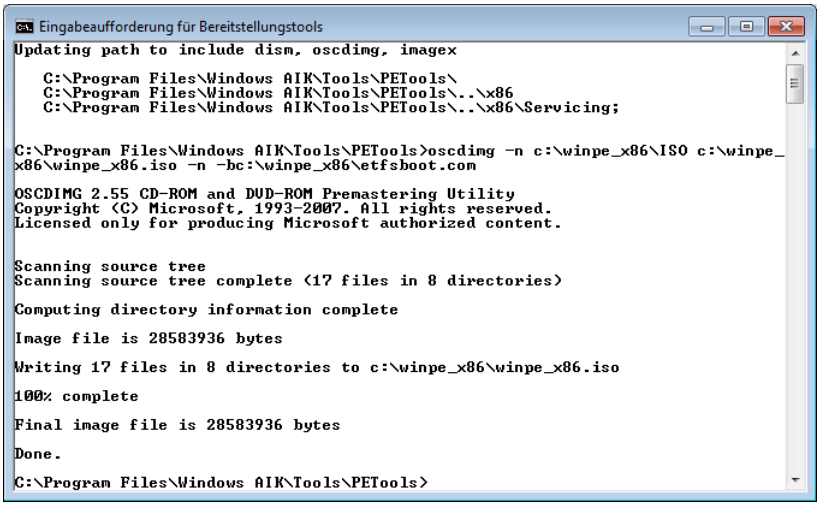

Eingabeaufforderung für Bereitstellungstools
Updating path to include dism, oscdimg, imagex
C:\Program Files\Windows AIK\Tools\PETools\
C:\Program Files\Windows AIK\Tools\PETools\..\x86
C:\Program Files\Windows AIK\Tools\PETools\..\x86\Servicing;
C:\Program Files\Windows AIK\Tools\PETools>oscdimg -n c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso -n -bc:\winpe_x86\etfsboot.com
OSCDIMG 2.55 CD-ROM and DVD-ROM Premastering Utility
Copyright (C) Microsoft, 1993-2007. All rights reserved.
Licensed only for producing Microsoft authorized content.
Scanning source tree
Scanning source tree complete (17 files in 8 directories)
Computing directory information complete
Image file is 28583936 bytes
Writing 17 files in 8 directories to c:\winpe_x86\winpe_x86.iso
100% complete
Final image file is 28583936 bytes
Done.
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 2.11 Erstellen eines Windows PE-ISO-Abbilds

10. Das ISO-Abbild liegt in *C:\Winpe_x86* und heißt *Winpe_x86.iso*. Brennen Sie die ISO-Datei auf einen CD- oder DVD-Rohling.

Übung 2 Erstellen eines WIM-Abbilds für den Computer *Canberra*

In dieser Übung starten Sie den Computer *Canberra* von dem Windows-Startdatenträger, den Sie in Übung 1 erstellt haben und der ImageX enthält. Dann erstellen Sie ein WIM-Abbild der Windows 7-Installation und speichern es (optional) in einer Netzwerkfreigabe.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Legen Sie im Computer *Canberra* das Windows PE-Medium ein und starten Sie den Computer neu.



Hinweis Ändern der BIOS-Startreihenfolge

Damit der Computer vom optischen Laufwerk startet, müssen Sie unter Umständen die Startreihenfolge im BIOS ändern. Drücken Sie dazu beim Systemstart die entsprechende Funktionstaste.

3. Windows PE startet und öffnet ein Eingabeaufforderungsfenster.
4. Zeichnen Sie mit dem Tool ImageX, das Sie auf Ihrem Windows PE-Medium bereitgestellt haben, ein Abbild der Referenzinstallation auf, indem Sie den Befehl **e:\imagex.exe /capture c: d:\Images\myimage.wim "Canberra Win7 install" /compress fast /verify** ausführen. Dieser Befehl zeichnet mithilfe des Tools ImageX, das auf dem CD/DVD-Laufwerk *E:* vorliegt, ein Abbild des Systemdatenträgers *C:* im Ordner *Images* auf der zweiten Festplatte *D:* auf. Sofern Sie andere Volumes verwenden, müssen Sie den Befehl entsprechend anpassen. Der Befehl benötigt einige Zeit; er listet Ordner (zum Beispiel den Papierkorb) auf, die nicht standardmäßig in das Abbild aufgenommen werden.
5. Geben Sie **exit** ein und entfernen Sie Ihren Windows PE-Startdatenträger. Der Computer startet nun unter Windows 7.
6. Prüfen Sie, ob die Datei *Myimage.wim* auf Laufwerk *D:* (oder dem Laufwerk, das Sie angegeben haben) vorhanden ist.
7. Wenn Sie das Abbild in einem Netzwerk freigeben wollen, können Sie eine Netzwerkfreigabe anlegen (zum Beispiel *\\Canberra\Images*), sie einem Netzlaufwerk (beispielsweise *Y:*) zuordnen und dann die WIM-Datei in diese Freigabe kopieren.

Zusammenfassung der Lektion

- Das in Windows 7 eingeführte Windows AIK stellt verschiedene Tools zum Erstellen von Systemabbildern zur Verfügung. Dazu gehören Windows SIM, ImageX, Oscdimg, DISM, USMT und diverse Windows PE-Tools.
- Mit Windows SIM erstellen Sie eine Antwortdatei für die unbeaufsichtigte Installation, die Sie anschließend benutzen, um mithilfe eines WIM-Abbilds einen Referenzcomputer einzurichten. Mit Sysprep bereiten Sie das Abbild vor. Anschließend starten Sie den Referenzcomputer unter Windows PE und zeichnen mit dem Tool ImageX das Abbild in einer WIM-Datei auf.

- WIM-Abbilder arbeiten auf Basis von Dateien. Sie können in einer VHD installiert oder für die Verteilung in einer Netzwerkfreigabe gespeichert werden. Sie können mehrere Abbilder in derselben WIM-Datei speichern.
- Mit dem Befehlszeilentool Sysprep bereiten Sie eine Windows-Installation auf die Abbilderstellung oder die Auslieferung an einen Benutzer vor. Vor allem verallgemeinern Sie mit diesem Tool ein Abbild und entfernen spezifische Daten wie die SID.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Aufzeichnen von Systemabbildern«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie erstellen ein WIM-Systemabbild einer Windows 7-Installation auf einem Referenzcomputer. Unter welchem Betriebssystem starten Sie den Computer und welches Windows AIK-Tool benutzen Sie?
   A. Sie starten unter Windows 7 und benutzen ImageX.
   B. Sie starten unter Windows 7 und benutzen Windows SIM.
   C. Sie starten unter Windows 7 und benutzen DISM.
   D. Sie starten unter Windows PE und benutzen ImageX.
   E. Sie starten unter Windows PE und benutzen Windows SIM.
   F. Sie starten unter Windows PE und benutzen DISM.
2. Sie erstellen eine Antwortdatei für eine automatische Windows 7-Installation. Was können Sie dafür benutzen? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Windows SIM aus dem Windows AIK
   B. Das Tool DISM aus dem Windows AIK
   C. Das MDT-Tool Deployment Workbench
   D. *Sysprep.exe*
   E. Windows-Editor
3. Sie wollen einen Referenzcomputer vorbereiten und sein Windows 7-Abbild für die Verteilung auf mehrere Zielcomputer vorbereiten. Sie möchten dabei Ihren eigenen Windows 7-Client als Administrationscomputer einsetzen. Welche der folgenden Aufgaben müssen Sie dafür ausführen? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Installieren Sie das Windows AIK auf Ihrem Administrationscomputer (sofern noch nicht vorhanden).
   B. Erstellen Sie mit Windows SIM eine Antwortdatei namens *Autounattend.xml* und speichern Sie diese Datei im Stammverzeichnis eines UFD.
   C. Installieren Sie Ihre gewünschte Windows 7-Edition auf dem Referenzcomputer.

D. Installieren Sie MDT 2010 auf Ihrem Administrationscomputer (sofern noch nicht vorhanden).
E. Erstellen Sie ein WDS-Aufzeichnungsabbild.
F. Erstellen Sie eine startfähige Windows PE-DVD, -CD oder -UFD (sofern noch nicht vorhanden).
G. Zeichnen Sie mit dem Tool ImageX ein Systemabbild des Referenzcomputers auf.
H. Bereiten Sie den Referenzcomputer mit Sysprep auf die Abbilderstellung vor.

4. Sie verwenden das Tool Sysprep, um eine Windows 7-Installation auf die Abbilderstellung vorzubereiten. Welche Befehlszeilenoption entfernt alle eindeutigen Systeminformationen aus der Installation?
   A. `/audit`
   B. `/oobe`
   C. `/generalize`
   D. `/unattend`
5. Welcher Konfigurationsdurchlauf des Windows-Setups wendet Einstellungen auf Windows 7 an, bevor die Windows-Willkommensseite startet?
   A. *oobeSystem*
   B. *auditSystem*
   C. *specialize*
   D. *offlineServicing*

Lektion 2: Verwalten von virtuellen Festplatten

Diese Lektion beschreibt, wie Sie native VHD-Dateien (Virtual Hard Disk) auf einem Windows 7-Computer erstellen und solche Dateien mit Tools wie Diskpart bereitstellen, ins Dateisystem einbinden, anfügen, trennen und löschen. Sie stellt außerdem startfähige VHD-Dateien vor und erklärt die Verwendung des Tools BCDEdit.

Die Lektion beschreibt, wie Sie mit dem Befehlszeilentool WIM2VHD (Windows Image to Virtual Hard Disk) aus einer Windows 7-Installationsquelle oder aus einem Abbild in einer benutzerdefinierten WIM-Datei VHD-Abbilder erstellen. Sie erfahren, wie Sie mit dem Offline Virtual Machine Servicing Tool das Abbild in einer VHD aktualisieren, das normalerweise offline ist, und wie Sie mit den Tools von WDS Abbilder verwalten und sie auf Clientcomputer sowie auf virtuelle Computer und VHDs exportieren, die online sind.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Erstellen, Bereitstellen im Dateisystem, Anfügen und Bereitstellen von VHD-Dateien und Erstellen einer startfähigen VHD
- Verwenden von Diskpart, BCDEdit und Datenträgerverwaltungstools
- Erstellen von VHD-Abbildern aus einer WIM-Datei mithilfe von WIM2VHD
- Beschreiben des Offline Virtual Machine Servicing Tools und der GUI- und Befehlszeilentools, die WDS zur Verfügung stellt

Veranschlagte Zeit für diese Lektion: 45 Minuten

Verwenden nativer VHDs in Windows 7

Das VHD-Format definiert eine VHD (virtuelle Festplatte), die in einer einzigen Datei enthalten ist. Eine VHD kann native Dateisysteme hosten und unterstützt alle üblichen Datenträgeroperationen. VHD-Dateien werden von Hyper-V, Virtual Server und Virtual PC für virtuelle Festplatten benutzt, die an einen virtuellen Computer angeschlossen sind. Das VHD-Dateiformat wird vom Microsoft Data Protection Manager, der Windows Server-Sicherung, der Clientcomputer-Sicherung (Windows Vista sowie Windows 7 Enterprise und Ultimate) und anderen Lösungen von Microsoft und anderen Herstellern benutzt.

In Windows 7 Enterprise oder Ultimate können Sie eine native VHD verwenden, um das laufende Betriebssystem zu hosten, ohne dass dazu andere übergeordnete Betriebssysteme oder virtuelle Computer gebraucht werden. Mit den Datenträgerverwaltungstools von Windows 7, zum Beispiel Diskpart und der Datenträgerverwaltung, können Sie eine VHD-Datei anlegen. Sie können ein Windows 7-WIM-Abbild in einer VHD bereitstellen und die VHD-Datei auf mehrere Systeme kopieren. Der Windows-Start-Manager kann so konfiguriert werden, dass er nativ vom VHD-Windows-Abbild startet.

Virtuelle Computer sind zwar allerorten im Einsatz, viele Unternehmensumgebungen werden aber nach wie vor auf physischen Computern betrieben. Es kann beispielsweise sein, dass Sie auf einem physischen Computer prüfen müssen, ob der Zugriff auf ein bestimmtes Hardwaregerät möglich ist. Als Enterpriseadministrator müssen Sie wahrscheinlich mehrere Arten von Abbildern verwalten, teils im WIM-Format für physische Computer und teils im VHD-Format für virtuelle Computer. Ein gemeinsames Abbildformat, das sowohl physische als auch virtuelle Computer unterstützt, bietet Flexibilität bei der Abbildbereitstellung und vereinfacht die Verwaltung der Abbilder.

In Windows 7 bedeutet native Unterstützung für das VHD-Format, dass VHD-Dateien erstellt und geändert werden können, ohne dass die Serverrolle *Hyper-V* installiert sein muss. VHD-Dateien können mithilfe der Datenträgerverwaltung verknüpft werden, und das Windows-Abbild innerhalb der VHD kann bearbeitet werden. Sie können die Windows-Bereitstellungstools im Windows AIK (vor allem ImageX und DISM) benutzen, um ein Windows-Abbild zu erstellen, das in einer VHD gespeichert wird, und dann Updates auf das Systemabbild in der VHD-Datei anzuwenden (nur in Windows 7 Ultimate und Enterprise Edition möglich).

Der native Systemstart von Windows 7 aus einer VHD-Datei setzt die Windows 7-Startumgebung voraus. Sie wird während einer vollständigen Betriebssysteminstallation initialisiert und umfasst den Windows-Start-Manager und Startkonfigurationsdaten (Boot Configuration Data, BCD).



Weitere Informationen Empfehlungen und Einschränkungen

Weitere Informationen über Empfehlungen und Einschränkungen zu VHDs finden Sie unter *http://technet.microsoft.com/en-us/library/dd440865.aspx*.



Hinweis Einschränkungen der verschiedenen Editionen

Nur Windows 7 Enterprise und Windows 7 Ultimate können gestartet werden, wenn sie in einer VHD installiert wurden. Dies wurde bereits erwähnt, Sie sollten es aber auf keinen Fall vergessen.

Erstellen einer nativen VHD

Windows 7 bietet native Unterstützung für VHDs. Früher wurden VHD-Dateien für Virtualisierungsplattformen wie Hyper-V, Virtual Server und Virtual PC eingesetzt, und diese Möglichkeit besteht weiterhin. In Windows 7 können Sie allerdings auch native VHDs auf nichtvirtuellen Computern erstellen.

In den Übungen am Ende dieser Lektion finden Sie Schritt-für-Schritt-Anleitungen, wie Sie eine native VHD anlegen und die VHD-Datei verknüpfen oder trennen. Der Rest dieses Abschnitts erklärt, wie dieser Vorgang im Prinzip abläuft.

Sie erstellen eine native VHD, indem Sie mit der rechten Maustaste auf *Computer* klicken und im Kontextmenü den Befehl *Verwalten* wählen, um die Computerverwaltung zu öffnen. Wählen Sie dort *Datenträgerverwaltung* aus. Klicken Sie mit der rechten Maustaste auf *Datenträgerverwaltung* und wählen Sie den Befehl *Virtuelle Festplatte erstellen*. Daraufhin öffnet sich das Dialogfeld *Virtuelle Festplatte erstellen und anfügen*. Wählen Sie hier den Speicherort aus, an dem Sie die VHD-Datei anlegen wollen (stellen Sie dabei sicher, dass genug Platz frei ist).

Im Allgemeinen legen Sie eine VHD auf einer zweiten internen oder externen Festplatte an (das ist aber nicht zwingend nötig). Dann geben Sie die Größe und die Formatierungseinstellungen der VHD an. Microsoft empfiehlt, die Standardeinstellung *Feste Größe* zu übernehmen, aber Sie können auch *Dynamisch erweiterbar* auswählen, wenn Sie nicht den gesamten Festplattenplatz reservieren wollen. Die Option *Feste Größe* liefert höhere Leistung und eignet sich daher besser für eine Produktivumgebung.

Sobald Sie auf *OK* klicken, wird eine neu angefügte (bereitgestellte) VHD erstellt. Initialisieren Sie diese Festplatte, indem Sie mit der rechten Maustaste auf das Symbol neben der

Datenträgerbezeichnung klicken und den Befehl *Datenträgerinitialisierung* wählen. Daraufhin öffnet sich das Dialogfeld *Datenträgerinitialisierung*. Wählen Sie hier die Partition aus und klicken Sie auf *OK*. Normalerweise brauchen Sie die Standardeinstellungen nicht zu ändern. Der Status des Datenträgers ändert sich nun auf *Online*.

Erstellen Sie ein neues einfaches Volume auf der VHD, indem Sie mit der rechten Maustaste auf *Nicht zugeordnet* klicken und den Befehl *Neues einfaches Volume* wählen. Daraufhin startet der Assistent zum Erstellen neuer einfacher Volumes. Geben Sie hier Größe, Dateisystem und Laufwerkbuchstaben an, tragen Sie eine Volumebezeichnung ein und klicken Sie auf *Fertig stellen*, um die VHD zu erstellen.

Anfügen und Trennen einer VHD

Sie können in der Datenträgerverwaltung auch eine VHD anfügen, damit Sie damit arbeiten können. Und Sie können die VHD wieder trennen, um ihre Eigenschaften zu ändern oder sie zu löschen. Wählen Sie in der Computerverwaltung den Zweig *Datenträgerverwaltung* aus, klicken Sie mit der rechten Maustaste auf *Datenträgerverwaltung* und wählen Sie den Befehl *Virtuelle Festplatte anfügen*. Daraufhin öffnet sich das Dialogfeld *Virtuelle Festplatte anfügen*. Klicken Sie auf *OK*, um die vorhandene VHD anzufügen. Falls Sie den Inhalt der VHD nicht verändern wollen (weil Sie beispielsweise ein Betriebssystem darauf installiert haben), können Sie das Kontrollkästchen *Schreibgeschützt* aktivieren.

Sie trennen eine VHD, indem Sie mit der rechten Maustaste auf das Symbol neben der Datenträgerbezeichnung klicken und den Befehl *Virtuelle Festplatte trennen* wählen. Nun wird das Meldungsfeld *Virtuelle Festplatte trennen* angezeigt. Klicken Sie auf *OK*, um die VHD zu trennen. Wollen Sie die VHD ganz löschen, nachdem sie getrennt wurde, können Sie das Kontrollkästchen *Datei für virtuelle Festplatte nach Entfernen des Datenträgers löschen* aktivieren.

Erstellen und Anfügen einer VHD mit dem Tool Diskpart

Sie können auch das Befehlszeilenprogramm Diskpart verwenden, um eine VHD anzulegen und anzufügen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie im Menü *Zubehör* mit der rechten Maustaste auf *Eingabeaufforderung* und wählen Sie den Befehl *Als Administrator ausführen*. Klicken Sie bei Bedarf auf *Ja*, um die Ausführung des Programms zu erlauben.
2. Geben Sie **diskpart** ein.
3. Geben Sie **create vdisk file=c:\win7\myothervhd.vhd maximum=20000** ein. Dieser Befehl erstellt eine VHD-Datei mit dem Namen *Myothervhd.vhd* mit einer Maximalgröße von 20 GByte in einem Ordner namens *Win7* auf dem Laufwerk *C:*. Sie können eine VHD auch auf einer zweiten internen Festplatte oder auf einer externen USB-Festplatte anlegen, sofern sie mit dem Dateisystem NTFS formatiert sind.
4. Geben Sie **select vdisk file=c:\win7\myothervhd.vhd** ein.
5. Geben Sie **attach vdisk** ein.
6. Geben Sie **create partition primary** ein.
7. Geben Sie **assign letter=v** ein.
8. Geben Sie **format quick label=Windows7** ein.
9. Geben Sie **exit** ein.

Damit wird die VHD-Datei *C:\Win7\Myothervhd.vhd* als primäre Partition angelegt. Abbildung 2.12 zeigt die Diskpart-Befehle zum Erstellen und Anfügen einer neuen VHD. In Abbildung 2.13 sehen Sie, wie die neu angefügte Festplatte in der Datenträgerverwaltung unter dem Laufwerkbuchstaben *V:* aufgelistet wird.

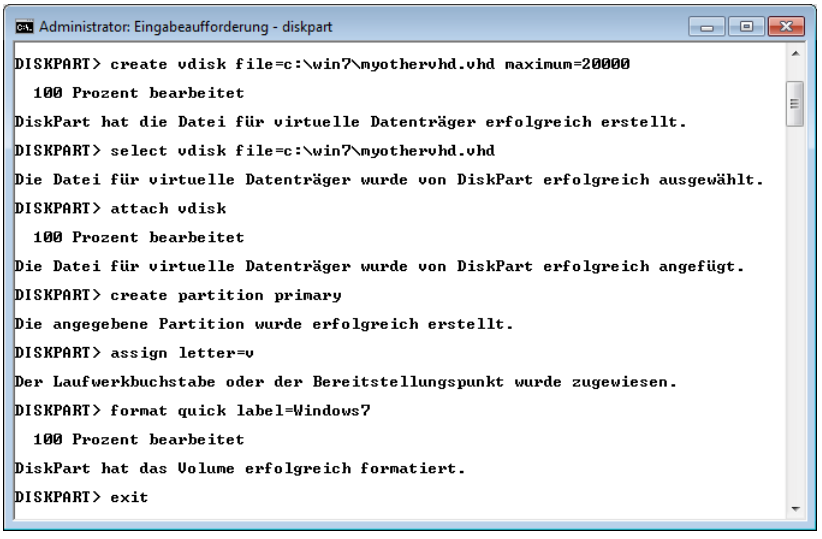

Administrator: Eingabeaufforderung - diskpart
DISKPART> create vdisk file=c:\win7\myothervhd.vhd maximum=20000
100 Prozent bearbeitet
DiskPart hat die Datei für virtuelle Datenträger erfolgreich erstellt.
DISKPART> select vdisk file=c:\win7\myothervhd.vhd
Die Datei für virtuelle Datenträger wurde von DiskPart erfolgreich ausgewählt.
DISKPART> attach vdisk
100 Prozent bearbeitet
Die Datei für virtuelle Datenträger wurde von DiskPart erfolgreich angefügt.
DISKPART> create partition primary
Die angegebene Partition wurde erfolgreich erstellt.
DISKPART> assign letter=v
Der Laufwerkbuchstabe oder der Bereitstellungspunkt wurde zugewiesen.
DISKPART> format quick label=Windows7
100 Prozent bearbeitet
DiskPart hat das Volume erfolgreich formatiert.
DISKPART> exit

Abbildung 2.12 Erstellen und Anfügen einer VHD

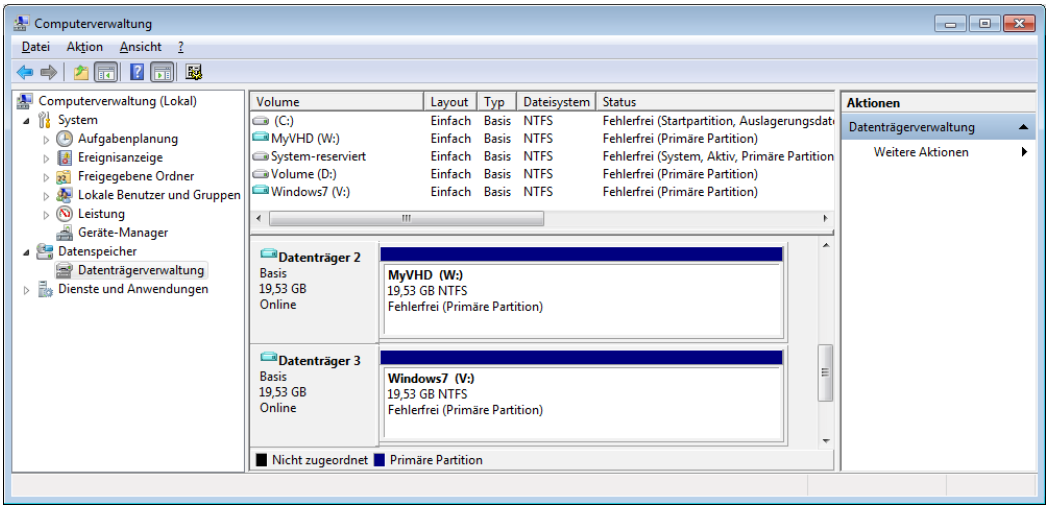


Abbildung 2.13 Die VHD wird in der Datenträgerverwaltung aufgelistet

Starten von einer VHD

Die Möglichkeit, von einer VHD zu starten (nur in den Windows 7-Editionen Ultimate und Enterprise), ist eines der leistungsfähigsten neuen Features, die in Windows 7 eingeführt wurden. Sie können den Computer so starten, als würde er von der primären Festplatte laufen, und Ihr Betriebssystem erkennt die gesamte Hardware, die in Ihrem System verfügbar ist. So

können Sie mehrere Betriebssysteme auf demselben Computer betreiben, ohne die Leistungsprobleme in Kauf nehmen zu müssen, die oft beim Einsatz virtueller PCs auftreten. Sie können mehrere VHDs mit unterschiedlichen installierten Betriebssystemen erstellen.

Weiter oben in dieser Lektion haben Sie gesehen, wie Sie eine neue VHD erstellen und sie in der Datenträgerverwaltung oder mit dem Tool Diskpart anfügen. Wenn Sie das Betriebssystem Windows 7 von der Produkt-DVD installieren wollen, brauchen Sie die Datei *Install.wim* von diesem Datenträger. Außerdem benötigen Sie das Tool ImageX (*Imagex.exe*). Wenn Sie, wie in Lektion 1 beschrieben, das Windows AIK installiert haben, finden Sie diese Datei in *C:\Program Files\Windows AIK\Tools\x86*.

Sie können auch ein WIM-Systemabbild, das Sie für Ihren Computer erstellt haben (wie in Lektion 1 beschrieben), auf eine VHD auf diesem Computer kopieren. Diese Schritte führen Sie in der Übung weiter unten in dieser Lektion durch.

Hinzufügen eines Systemstarteintrags für eine VHD-Datei

Sobald Sie eine VHD erstellt und ein Systemabbild darauf installiert haben, können Sie mit dem Tool BCDEdit (*Bcdedit.exe*) einen Starteintrag für die VHD-Datei zu Ihrem Windows 7-Computer hinzufügen. Eine Schritt-für-Schritt-Anleitung dazu enthält die Übung weiter unten in dieser Lektion. Dieser Abschnitt beschreibt, wie der Vorgang prinzipiell abläuft:

Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben Sie einen Befehl ein, der ähnlich wie der folgende aussieht:

bcdedit /copy {current} /d "Beschreibung Ihrer neuen VHD"

Dieser Befehl gibt die GUID des Ladeobjekts zurück. In den folgenden Befehlen ersetzen Sie die Variable `<GUID>` durch diesen Wert:

bcdedit /set <*GUID*> device vhd=[*Laufwerkbuchstabe*:]\<*Verzeichnis*>\<*VHD-Dateiname*>
bcdedit /set <*GUID*> osdevice vhd=[*Laufwerkbuchstabe*:]\<*Verzeichnis*>\<*VHD-Dateiname*>

BCDEdit sucht die VHD-Datei, und Bootmgr sucht die Partition, in der die VHD-Datei liegt, um daraus zu starten. Geben Sie zuletzt den folgenden Befehl ein:

bcdedit /set <*GUID*> detecthal on

Das Argument `detecthal` zwingt Windows 7, die HAL (Hardware Abstraction Layer) automatisch zu erkennen. Der folgende Befehl prüft, ob Ihr Starteintrag richtig erstellt wurde:

bcdedit /v

Verwenden Sie den folgenden Befehl, wenn Sie einen vorhandenen VHD-Eintrag aus dem Systemstartmenü löschen wollen:

bcdedit /delete <*GUID*> /cleanup

Damit löschen Sie den angegebenen Betriebssystemeintrag aus dem Speicher und entfernen den Eintrag aus dem angezeigten Menü.

Wenn Sie Ihren Computer neu starten, nachdem Sie diese Schritte richtig ausgeführt haben, müssten Sie einen zusätzlichen Eintrag im Systemstartmenü sehen, der den Standardeintrag für das Betriebssystem Windows 7 ergänzt.



Weitere Informationen BCDEdit

Weitere Informationen über BCDEdit erhalten Sie, wenn Sie auf *http://msdn.microsoft.com/en-us/library/aa906217.aspx* im Navigationsfensterabschnitt den Knoten *BCD Boot Options Reference* aufklappen und auf die Links klicken.



Prüfungstipp

Sie können *Bcdedit.exe* verwenden, um eine VHD-Datei als Systemstartoption einzutragen. Aber Sie können mit diesem Tool keine VHD-Dateien erstellen.

Verwenden des Tools WIM2VHD

Mit dem Befehlszeilentool WIM2VHD (Windows Image to Virtual Hard Disk) erstellen Sie VHD-Abbilder aus beliebigen Windows 7-Installationsquellen oder aus einem Abbild in einer angepassten WIM-Datei. WIM2VHD erstellt VHDs, die direkt in die OOBE-Oberfläche (Out-of-Box-Experience) starten. Sie können die OOBE-Konfiguration auch automatisieren, indem Sie Ihre eigene *Unattend.xml*-Datei zur Verfügung stellen.

Sie brauchen einen Windows 7-Clientcomputer, auf dem das Windows AIK installiert ist, sowie ein Betriebssystemabbild in einer WIM-Datei. Außerdem müssen Sie eine native VHD auf diesem Computer erstellt haben.

Das Tool WIM2VHD wird über Cscript ausgeführt. Die Syntax lautet:

```
cscript wim2vhd.wsf. /wim:<WIM-Pfad> /sku:<Sku> [/vhd:<VHD-Pfad>] [/size:<VHD-Größe_in_MByte>] [/disktype:<dynamic|fixed>] [/unattend:<Unattendxml-Pfad>] [/qfe:<qfe1,.,qfen>] [/hyperv:<true|false>] [/ref:<ref1,.,refn] [/dbg:<Argumente>] [/passthru:<Physisches Laufwerk>])
```

Argumente von WIM2VHD

Tabelle 2.8 beschreibt die Argumente des Tools WIM2VHD.

Tabelle 2.8 Argumente von WIM2VHD

Argument	Beschreibung
`/wim:<WIM-Pfad>`	Dies ist der Pfad der WIM-Datei, die Sie zum Erstellen der VHD benutzen.
`/sku:<SKU-Name>|<SKU-Index>`	Die SKU (Stock-Keeping Unit) gibt an, welche Edition des Betriebssystems beim Erstellen der VHD benutzt wird (zum Beispiel »HomePremium«). Sie können auch eine Nummer angeben, die Sie erhalten, indem Sie mit ImageX die gewünschte WIM-Datei analysieren.
`/vhd:<VHD-Pfad>` (optional)	Definiert den Pfad und den Namen der VHD, die erstellt wird. Ist bereits eine Datei dieses Namens vorhanden, wird sie überschrieben. Falls kein VHD-Pfad angegeben ist, wird sie im aktuellen Ordner angelegt. ▶

Argument	Beschreibung
/size:<*VHD-Größe_in_MByte*> (optional)	Bei virtuellen Festplatten fester Größe ist dies die Größe der erstellten VHD in MByte. Bei einer dynamisch erweiterbaren Festplatte ist es die Maximalgröße in MByte, die angibt, wie groß die VHD höchstens werden kann, wenn mehr Platz gebraucht wird. Falls Sie keinen Wert für diesen Parameter angeben, wird der Standardwert 40 GByte verwendet.
/disktype:<dynamic|fixed> (optional)	Legt fest, welche Art von VHD erstellt wird: dynamisch erweiterbar oder feste Größe. Ein Datenträger fester Größe reserviert direkt beim Erstellen den gesamten Festplattenplatz für die VHD. Ein dynamisch erweiterbarer Datenträger belegt immer nur so viel Platz, wie die in der VHD gespeicherten Dateien einnehmen; wird mehr Platz benötigt, wächst die Datei. Der Standardwert ist dynamic.
/unattend:<*Unattendxml-Pfad*> (optional)	Gibt den Pfad zu einer *Unattend.xml*-Datei an, die benutzt wird, um die OOBE-Phase des Windows-Setups zu automatisieren, wenn die VHD zum ersten Mal gestartet wird.
/qfe:<*qfe1,.,qfen*> (optional)	Eine kommagetrennte Liste mit QFE- (Quick Fix Engineering) oder Hotfixpatches, die auf die VHD angewendet werden, sobald die WIM implementiert ist.
/ref:<*ref1,.,refn*> (optional)	Eine kommagetrennte Liste mit WIM-Teildateien, die auf die VHD angewendet werden. Eine WIM-Teildatei entsteht beim Aufteilen einer WIM, üblicherweise hat sie die Dateierweiterung *.swm*. Der erste Teil der aufgeteilten WIM sollte im Argument /wim angegeben werden. Die weiteren Teile werden (in der richtigen Reihenfolge) mit /ref aufgelistet.
/dbg:<*Protokoll*>,<*Port/Kanal/Ziel*>[,<*Baudrate*>]. (optional)	Konfiguriert das Debugging für das Betriebssystem auf der VHD.

Sie können bei diesem Vorgang Ihre eigenen, angepassten WIM-Dateien verwenden. Seien Sie aber vorsichtig: Microsoft unterstützt zwar den zugrunde liegenden Prozess, wie im Windows AIK dokumentiert, aber für WIM2VHD wird momentan kein Support geboten.

Sie können Dateien von Hand in die VHD kopieren, es gibt aber keine Möglichkeit, dies mit WIM2VHD zu erledigen.

Beispiele für die Verwendung von WIM2VHD

Sie erstellen eine VHD, die Windows 7 Ultimate enthält und eine *Unattend.xml*-Antwortdatei für das automatisierte Setup verwendet, indem Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen und den folgenden Befehl ausführen:

cscript wim2vhd.wsf /win:x:\mysources\install.wim /sku: ultimate /unattend: C:\answer_files\unattend.xml

Sie brauchen lediglich den Speicherort der WIM-Datei und der Antwortdatei an Ihr eigenes System anzupassen.

Wenn Sie die WIM-Datei mit ImageX analysiert haben und wissen, dass die SKU (Edition) innerhalb der WIM den Index 1 hat, können Sie das erste Abbild in einer benutzerdefinierten WIM im Ordner *C:\Mystuff* auf eine VHD namens *Mycustom.vhd* anwenden, indem Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen und diesen Befehl eingeben:

cscript wim2vhd.wsf /wim:C:\mystuff\custom.wim /sku:1 /VHD:C:\mycustom.vhd



Weitere Informationen WIM2VHD

Weitere Informationen über WIM2VHD finden Sie unter *http://code.msdn.microsoft.com/wim2vhd*.

Aktualisieren einer VHD mit dem Offline Virtual Machine Servicing Tool

Das Offline Virtual Machine Servicing Tool 2.0.1 ist ein sogenannter Solution Accelerator (wie auch MDT 2010). Neben den benötigten Installationsdateien stellt ein *Solution Accelerator* automatisierte Tools und zusätzliche Anleitungsdateien zur Verfügung. Sie können das Tool auf einem Server installieren, der unter Windows Server 2008 oder Windows Server 2003 SP2 läuft. Dort arbeitet es in Kombination mit Microsoft System Center Virtual Machine Manager (SCVMM) 2007 oder SCVMM 2008, um virtuelle Computer und VHDs offline zu verwalten.

Wenn Ihr Server im selben Netzwerk liegt wie ein Client mit Windows 7 Enterprise oder Ultimate, auf dem Sie eine startfähige VHD konfiguriert haben, können Sie mithilfe dieses Tools den VHD-Inhalt bearbeiten, während die VHD offline ist. Startet Ihr Windows 7-Computer normalerweise nicht von der VHD, erhält die Offline-VHD keine Betriebssystemupdates. Das Tool bietet die Möglichkeit, die VHD auf dem neusten Stand zu halten, sodass beim Systemstart von der VHD keine Sicherheitslücken in Ihrem Computer auftreten.

Das Offline Virtual Machine Servicing Tool kann so konfiguriert werden, dass es den Clientcomputer gerade so lange von VHD startet, bis die VHD alle Updates von SCCM 2007 oder Windows Server Update Services (WSUS) erhalten hat. Sobald das Betriebssystem der VHD auf dem neusten Stand ist, startet das Tool den Clientcomputer wieder von seinem normalen Startdatenträger.

Das Offline Virtual Machine Servicing Tool umfasst folgende Features:

- Kurze Einführung
- Installationsdatei *OfflineVMServicing_x64.msi*
- Installationsdatei *OfflineVMServicing_x86.msi*
- Anleitung für die ersten Schritte mit Offline Virtual Machine Servicing Tool (*Getting Started Guide*)
- Versionshinweise in *Offline_VM_Servicing_Tool_2.0_Release_Notes*
- Hilfedatei *Offline_Virtual_Machine_Servicing_Tool_Help*

Das Tool verwendet eine Wartungsaufgabe, die Sie in der Windows-Aufgabenplanung auf dem Server konfigurieren, um die Updateoperation zu verwalten. Der Wartungsauftrag startet den Clientcomputer von der VHD, löst den benötigten Softwareupdatezyklus unter Rückgriff auf SCCM oder WSUS aus und startet den Clientcomputer schließlich von seinem normalen Startdatenträger neu.

Installieren des Offline Virtual Machine Servicing Tools

Sie können das Offline Virtual Machine Servicing Tool erst installieren, wenn Sie SCVMM bereitgestellt haben. (Sie können das Tool allerdings herunterladen und die Dokumentation lesen.) Eine Betaversion von SCVMM 2008 ist momentan unter *http://www.microsoft.com/systemcenter/scvmm/downloadbeta.mspx* erhältlich. Die SCVMM-Dokumentation erhalten Sie aus derselben Quelle. Beachten Sie, dass das Offline Virtual Machine Servicing Tool und SCVMM Servertools sind. Sie können sie nicht auf einem Windows 7-Computer installieren.

Sie können die Installationsdateien und die zugehörige Dokumentation des Offline Virtual Machine Servicing Tools direkt von *http://www.microsoft.com/downloads/details.aspx?FamilyID=8408ecf5-7afe-47ec-a697-eb433027df73&DisplayLang=en* herunterladen. Wahrscheinlich ist es allerdings einfacher, die Seite *http://technet.microsoft.com/en-us/library/cc501231.aspx* aufzurufen und auf den Link am Ende der Webseite zu klicken. Alle Dateien werden in Form einer einzigen komprimierten Datei heruntergeladen, die Sie anschließend in einen Ordner entpacken, den Sie für diesen Zweck auf dem Server angelegt haben. Sie sollten erst die *Release Notes* und den *Getting Started Guide* lesen, um sich mit dem Tool vertraut zu machen, bevor Sie die Installationsdatei ausführen.

Die Administratorkonsole von SCVMM

SCVMM stellt eine Verwaltungslösung für das virtualisierte Datencenter zur Verfügung, die Ihnen hilft, eine Infrastruktur für die zentralisierte IT-Verwaltung aufzubauen, die Serverauslastung zu steigern und die dynamische Ressourcennutzung über mehrere Virtualisierungsplattformen hinweg zu optimieren. Es arbeitet mit dem Offline Virtual Machine Servicing Tool zusammen, um sicherzustellen, dass virtuelle Computer und VHDs auf dem neusten Stand bleiben. SCVMM bietet folgende Features:

- Es verwaltet virtuelle Computer, die unter Windows Server 2008 Hyper-V und Microsoft Hyper-V Server laufen.
- Es unterstützt die Virtualisierung von Computern, die unter Virtual Server und VMware ESX Server laufen.
- Es bietet Endpunkt-zu-Endpunkt-Unterstützung für die Konsolidierung physischer Server in einer virtuellen Infrastruktur.
- Es bietet Leistungs- und Ressourcenoptimierung (Performance and Resource Optimization, PRO) für die dynamische Verwaltung einer virtuellen Infrastruktur.
- Es implementiert die Verteilung virtueller Workloads auf die am besten geeigneten physischen Hostserver.
- Es stellt eine vollständige Bibliothek zur Verfügung, in der Sie alle Bausteine Ihres virtuellen Datencenters zentral verwalten.

Die SCVMM-Administratorkonsole (Abbildung 2.14) baut auf einer Windows PowerShell-Befehlszeilenschnittstelle auf. Alle Aktionen in der Administratorkonsole können auch in der Windows PowerShell-Befehlszeile ausgeführt werden, und jeder Assistent in der Benutzeroberfläche zeigt die entsprechenden Befehlszeilenaktionen an. Die Administratorkonsole integriert sich in System Center Operations Manager 2007, sodass Sie auch Daten zur physischen Umgebung erhalten, nicht nur zur virtuellen.

Bereitstellen in einer Online-VHD mithilfe der Windows-Bereitstellungsdienste

Mit den Windows-Bereitstellungsdiensten (Windows Deployment Services, WDS) können Sie Windows 7 Enterprise oder Ultimate im Remotezugriff auf den startfähigen VHDs beliebiger Clientcomputer bereitstellen. Lektion 1 dieses Kapitels hat WDS-Abbilder bereits kurz erwähnt. Sie können die WDS-Dokumentation (in englischer Sprache) mit *Getting Started Guide*, *Deployment Guide* und WDSUTIL-Befehlszeilensyntax unter *http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3cb929bc-af77-48d2-9b51-48268cd235fe* herunterladen. Eine Schritt-für-Schritt-Anleitung finden Sie unter *http://*

www.microsoft.com/downloads/details.aspx?familyid=14CA18B1-B433-4F62-8586-B0A2096460EB&displaylang=en. Unter *http://technet.microsoft.com/de-de/library/cc771670%28WS.10%29.aspx* können Sie eine deutsche Version der Schritt-für-Schritt-Anleitung online lesen.

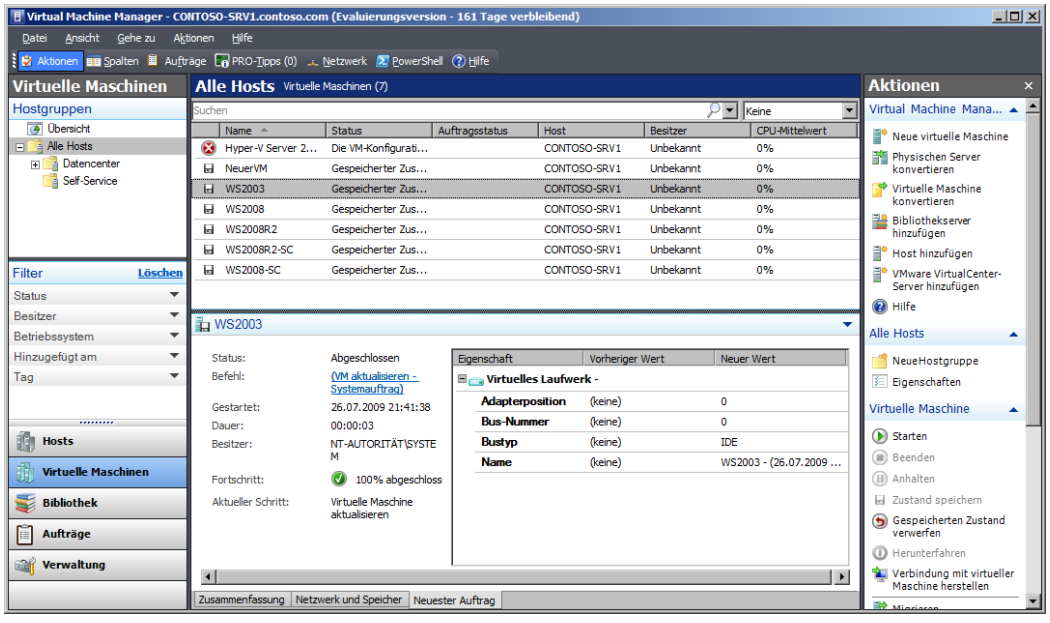


Abbildung 2.14 Die SCVMM-Administratorkonsole

Wenn Sie Windows 7-Abbilder mit WDS verteilen wollen, sollten Sie es auf einem Server installieren, der unter Windows Server 2008 oder Windows Server 2008 R2 läuft. WDS ist eine Serverrolle, und Sie können es im Fenster *Aufgaben der Erstkonfiguration*, im Server-Manager oder mit dem Befehlszeilenprogramm ServerManagerCmd installieren.



Weitere Informationen Voraussetzungen für die WDS-Installation

Weitere Informationen darüber, welche Voraussetzungen erfüllt sein müssen, damit Sie WDS installieren und benutzen können, finden Sie unter *http://technet.microsoft.com/de-de/library/cc771670(WS.10).aspx*.

WDS verringert die Komplexität von Bereitstellungen und senkt die Kosten gegenüber einer manuellen Installation. Sie können damit Windows-Betriebssysteme, darunter auch Windows 7, über das Netzwerk auf Zielcomputern, virtuellen Computern im Onlinestatus und Online-VHDs installieren. WDS greift auf Standardsetuptechnologien von Windows Server 2008 zurück, darunter Windows PE, WIM-Dateien und abbildbasiertes Setup.

WDS stellt das MMC-Snap-In *Windows-Bereitstellungsdienste* als GUI-Tool und das Befehlszeilentool WDSUTIL zur Verfügung. In der Konsole können Sie praktisch alle Bereitstellungsaufgaben erledigen, allerdings ist es nicht möglich, darin die Vorabbereitstellung (Pre-Staging) für Clientcomputer durchzuführen. Sie können damit aber die Richtlinie zum

automatischen Hinzufügen von Clients einstellen und ausstehende Computer genehmigen oder zurückweisen.

Mit dem Befehlszeilentool WDSUTIL können Sie alle Bereitstellungsaufgaben durchführen. WDSUTIL eignet sich auch, um häufig benötigte Aufgaben mit Skripts zu automatisieren und die erforderlichen Befehle in einfachen Batchdateien auszuführen; keiner der WDS-UTIL-Befehle benötigt eine interaktive Benutzersitzung.



Weitere Informationen Konfigurieren Ihrer Bereitstellung

Weitere Informationen über das Konfigurieren einer Bereitstellung mit WDS finden Sie unter *http://technet.microsoft.com/de-de/library/cc732529(WS.10).aspx*.



Weitere Informationen WDS-Bereitstellungsszenarien

Eine Beschreibung der Szenarien, in denen der Einsatz von WDS sinnvoll ist, enthält *http://technet.microsoft.com/de-de/library/cc770667.aspx*.

Schnelltest

1. Welche Verwaltungstools stellt WDS zur Verfügung?
2. Mit welchen dieser Tools können Sie die Vorabbereitstellung eines Clientcomputers ausführen?

Antworten zum Schnelltest

1. Das MMC-Snap-In *Windows-Bereitstellungsdienste* als GUI-Tool und das Befehlszeilentool WDSUTIL
2. Nur mit dem Befehlszeilentool WDSUTIL

Verwenden von WDS-Abbildern

WDS verwendet ein Verfahren mit aufgeteilten WIM-Abbildern, bei dem Dateiressourcen von allen Abbildgruppen gemeinsam verwendet werden. Die Metadaten jedes Abbilds liegen in einer separaten Abbilddatei. Der WDS-Abbildspeicher erstellt einen Satz mit aufgeteilten Medien, der zwei Dateien umfasst:

- Eine einfache WIM-Datei, die lediglich die Definition des Abbilds enthält
- Die Datei *Res.rwm*, die alle Dateiressourcen für alle Abbilder in der Abbildgruppe enthält; die Daten in *Res.rwm* liegen im Einzelinstanzformat vor und sind komprimiert

An diesem Punkt ist es sinnvoll, noch einmal kurz auf den Unterschied zwischen einem Installationsabbild und einem Startabbild einzugehen. Installationsabbilder sind die Betriebssystemabbilder, die Sie auf dem internen Datenträger, auf einem startfähigen externen Datenträger oder auf startfähigen VHDs des Clientcomputers bereitstellen. Startabbilder sind dagegen die Abbilder, unter denen Sie einen Clientcomputer starten, um die Betriebssysteminstallation auszuführen. Startabbilder enthalten Windows PE und die *Setup.exe* für den WDS-Client mit den zugehörigen WDS-Dateien. Sie können zu diesem Zweck die Standardstartabbilder, die auf den Windows 7- oder Windows Server 2008 R2-Medien enthalten sind, unverändert übernehmen.



Weitere Informationen WDS-Dokumentation

Sie können die WDS-Dokumentation (in englischer Sprache) inklusive einer Schritt-für-Schritt-Anleitung unter *http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3cb929bc-af77-48d2-9b51-48268cd235fe* herunterladen. Dies ist ein Link in den Windows Server 2008-Bereich, weil WDS eine Serverrolle ist, die nicht auf einem Clientcomputer installiert werden kann. Unter *http://technet.microsoft.com/de-de/library/cc771670%28WS.10%29.aspx* können Sie eine deutsche Version der Schritt-für-Schritt-Anleitung online lesen.

Wenn Sie die WDS-Serverrolle auf Ihrem Bereitstellungsserver installieren, steht auch das Befehlszeilentool WDSUTIL zur Verfügung. Sie können entweder das MMC-Snap-In *Windows-Bereitstellungsdienste* oder WDSUTIL verwenden, um Startabbilder aus der WIM-Datei zu erstellen, die Sie einer geeigneten Betriebssystem-DVD entnehmen.

Erstellen eines Aufzeichnungsabbilds

Gehen Sie folgendermaßen vor, um auf Ihrem WDS-Server im MMC-Snap-In *Windows-Bereitstellungsdienste* ein Aufzeichnungsabbild zu erstellen:

1. Erweitern Sie im MMC-Snap-In *Windows-Bereitstellungsdienste* den Knoten *Startabbilder*.
2. Klicken Sie mit der rechten Maustaste auf das Abbild, das Sie als Aufzeichnungsabbild verwenden wollen (üblicherweise die Datei *\Sources\Boot.wim* vom Installationsmedium).
3. Wählen Sie im Kontextmenü den Befehl *Aufzeichnungsstartabbild erstellen*.
4. Geben Sie einen Namen, eine Beschreibung und den Speicherort ein, an dem Sie eine lokale Kopie der Datei ablegen wollen. Dieser Speicherort ist wichtig, damit Sie eine lokale Kopie haben, falls während der Bereitstellung des Aufzeichnungsabbilds ein Netzwerkproblem auftritt.
5. Folgen Sie den Anweisungen im Assistenten. Klicken Sie auf *Fertig stellen*, wenn Sie alle Eingaben vorgenommen haben.
6. Klicken Sie mit der rechten Maustaste auf den Ordner *Startabbilder*.
7. Wählen Sie im Kontextmenü den Befehl *Startabbild hinzufügen*.
8. Wählen Sie das neue Aufzeichnungsabbild aus und klicken Sie auf *Weiter*.
9. Folgen Sie den Anweisungen im Assistenten zum Erstellen von Aufzeichnungsabbildern.

Gehen Sie folgendermaßen vor, um mit WDSUTIL ein Aufzeichnungsabbild zu erstellen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **wdsutil /New-CaptureImage /Image:<*Quellstartabbild*> /Architecture:{x86|ia64|x64} /DestinationImage /FilePath:<*Dateipfad*>** ein, wobei `<Dateipfad>` Pfad und Name für das Aufzeichnungsabbild ist.

Hinzufügen eines Startabbilds

Gehen Sie folgendermaßen vor, um auf Ihrem WDS-Server im MMC-Snap-In *Windows-Bereitstellungsdienste* ein Startabbild zum WDS-Abbildspeicher hinzuzufügen:

1. Klicken Sie mit der rechten Maustaste auf den Knoten *Startabbilder* und wählen Sie den Befehl *Startabbild hinzufügen*.
2. Geben Sie den Pfad des Startabbilds ein oder wählen Sie die Abbilddatei aus, und klicken Sie auf *Weiter*. Normalerweise verwenden Sie das unveränderte Standardstartabbild, das auf dem Installationsmedium des Windows Server-Betriebssystems enthalten ist.
3. Geben Sie einen Namen und eine Beschreibung für das Abbild ein und klicken Sie auf *Weiter*.
4. Prüfen Sie Ihre Einstellungen und klicken Sie auf *Weiter*.

Gehen Sie folgendermaßen vor, um ein Startabbild mit WDSUTIL hinzuzufügen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **WDSUTIL /Verbose /Progress /Add-Image /ImageFile:<*Pfad*> /ImageType:Boot** ein, wobei *<Pfad>* der vollständige Pfad zur Abbilddatei ist.

Erstellen eines Suchabbilds

Gehen Sie folgendermaßen vor, um auf Ihrem WDS-Server im MMC-Snap-In *Windows-Bereitstellungsdienste* ein Suchabbild zu erstellen:

1. Erweitern Sie im MMC-Snap-In *Windows-Bereitstellungsdienste* den Knoten *Startabbilder*.
2. Klicken Sie mit der rechten Maustaste auf das Abbild, das Sie als Suchabbild verwenden wollen. Üblicherweise ist das die Datei *Boot.wim* aus dem Verzeichnis *\Sources* der Installations-DVD des Betriebssystems.
3. Wählen Sie im Kontextmenü den Befehl *Suchabbild erstellen*.
4. Folgen Sie den Anweisungen im Assistenten zum Erstellen von Suchabbildern. Klicken Sie auf *Fertig stellen*, wenn Sie alle Eingaben vorgenommen haben.

Gehen Sie folgendermaßen vor, um mit WDSUTIL ein Suchabbild zu erstellen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **WDSUTIL /New-DiscoverImage /Image:<*Name*> /Architecture:{x86|x64|ia64} /DestinationImage /FilePath:<*Pfad und Name der neuen Datei*>** ein. Mit welchem Server das Suchabbild eine Verbindung herstellt, können Sie festlegen, indem Sie **/WDSServer:<*Servername oder -IP*>** anhängen.

Hinzufügen eines Installationsabbilds

Gehen Sie folgendermaßen vor, um auf Ihrem WDS-Server im MMC-Snap-In *Windows-Bereitstellungsdienste* ein Installationsabbild zum WDS-Abbildspeicher hinzuzufügen:

1. Klicken Sie in der Konsole *Windows-Bereitstellungsdienste* mit der rechten Maustaste auf *Installationsabbilder* und wählen Sie den Befehl *Installationsabbild hinzufügen*.
2. Wählen Sie eine Abbildgruppe aus.
3. Wählen Sie die Datei aus, die Sie hinzufügen wollen.
4. Gehen Sie die übrigen Seiten des Assistenten durch.

Gehen Sie folgendermaßen vor, um mit WDSUTIL ein Installationsabbild hinzuzufügen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **WDSUTIL /Add-ImageGroup /ImageGroup:<*Name der Abbildgruppe*>** ein, falls Sie eine Abbildgruppe anlegen müssen.
3. Geben Sie **WDSUTIL /Verbose /Progress /Add-Image /ImageFile:<*Pfad zur .wim-Datei*> /ImageType:Install** ein.

Sofern es auf dem Server mehrere Abbildgruppen gibt, können Sie **/ImageGroup:<*Abbildgruppenname*>** anhängen, um anzugeben, zu welcher Gruppe das Abbild hinzugefügt werden soll. Wenn Sie in Schritt 3 **/SkipVerify** an den Befehl anhängen, wird die Integritätsprüfung vor dem Hinzufügen des Abbilds übersprungen.

Exportieren eines Abbilds

Wenn Sie ein Startabbild exportieren, kopiert WDS die Datei in das angegebene Ziel. Wenn Sie ein Installationsabbild exportieren, fasst WDS die Metadaten aus der Datei *Install.wim* mit den Ressourcen in der Datei *Res.rwm* zu einer einzigen WIM-Datei zusammen, die am angegebenen Ziel gespeichert wird.

Gehen Sie folgendermaßen vor, um auf Ihrem WDS-Server im MMC-Snap-In *Windows-Bereitstellungsdienste* ein Start- oder Installationsabbild aus Ihrem Server auf eine Festplatte oder eine startfähige VHD auf einem Clientcomputer zu exportieren:

1. Klicken Sie mit der rechten Maustaste auf das Start- oder Installationsabbild und wählen Sie den Befehl *Abbild exportieren*.
2. Wählen Sie im Dialogfeld einen Dateinamen und den Netzwerkpfad aus, in den das Abbild exportiert werden soll.

Gehen Sie folgendermaßen vor, um mit WDSUTIL ein Start- oder Installationsabbild aus Ihrem Server auf eine Festplatte oder eine startfähige VHD auf einem Clientcomputer zu exportieren:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **WDSUTIL /Verbose /Progress /Export-Image /Image:<*Name*> /ImageType:Boot /Architecture:{x86|x64|ia64} /DestinationImage /Filepath: <*Pfad und Dateiname*>** ein, wenn Sie ein Startabbild exportieren wollen.
3. Geben Sie **WDSUTIL /Verbose /Progress /Export-Image /Image:<*Name*> /ImageType:Install /ImageGroup:<*Abbildgruppenname*> /DestinationImage /Filepath:<*Pfad und Dateiname*>** ein, wenn Sie ein Installationsabbild exportieren wollen.

Sie können **/Name:<*Name*>** oder **/Description:<*Beschreibung*>** an den Befehl anhängen, wenn Sie diese Metadatenfelder im Abbild mit Werten füllen wollen. Das Verhalten für den Fall, dass das in `/DestinationImage` angegebene Abbild bereits vorhanden ist, legen Sie mit **/Overwrite:{Yes|No|Append}** fest. `Yes` überschreibt das Abbild, `No` löst einen Fehler aus und `Append` (nur bei Installationsabbildern verfügbar) hängt das neue Abbild an die vorhandene WIM-Datei an.

Aktualisieren eines Abbilds

Gehen Sie folgendermaßen vor, um auf Ihrem WDS-Server im MMC-Snap-In *Windows-Bereitstellungsdienste* ein Abbild durch eine aktualisierte Version zu ersetzen:

1. Klicken Sie mit der rechten Maustaste auf das Start- oder Installationsabbild und wählen Sie den Befehl *Abbild ersetzen*.
2. Wählen Sie das aktualisierte Abbild aus.
3. Schließen Sie den Assistenten ab.

Gehen Sie folgendermaßen vor, um mit WDSUTIL ein Abbild auf dem Server durch eine aktualisierte Version zu ersetzen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **WDSUTIL /Verbose /Progress /Replace-Image /Image:<*Name*> /ImageType:Boot /Architecture:{x86|x64|ia64} /ReplacementImage /ImageFile: <*Pfad*>** ein, wenn Sie ein Startabbild ersetzen wollen.
3. Geben Sie **WDSUTIL /Verbose /Progress /Replace-Image /Image:<*Name*> /ImageType:Install /ImageGroup:<*Abbildgruppenname*> /ReplacementImage /ImageFile:<*Pfad*>** ein, wenn Sie ein Installationsabbild ersetzen wollen.

Bei diesen Schritten wird das neue Abbild zum Abbildspeicher hinzugefügt, und das alte wird gelöscht. Sie können das neue Abbild anschließend auf Zielcomputer, virtuelle Computer im Onlinestatus oder Online-VHDs exportieren.



Prüfungstipp

Sie können WIM-Abbilder auf beschreibbaren Medien aktualisieren, sie zu einem WDS-Abbildspeicher hinzufügen und auf die gewünschten Zielcomputer, virtuellen Computer im Onlinestatus und Online-VHDs exportieren. Wenn Sie allerdings virtuelle Computer, die offline sind, oder VHDs regelmäßig »aufwecken« wollen, damit sie Updates von WSUS (oder auf anderen Wegen) erhalten, brauchen Sie das Offline Virtual Machine Servicing Tool, das weiter oben in dieser Lektion vorgestellt wurde.



Weitere Informationen Verwalten von Abbildern mit WDS

Weitere Informationen, wie Sie Abbilder mithilfe von WDS verwalten, finden Sie unter *http://technet.microsoft.com/de-de/library/cc732961.aspx*. Dort wird unter anderem erklärt, wie Sie Abbildattribute festlegen und anzeigen, ein Abbild entfernen, eine Abbildgruppe hinzufügen oder löschen und Informationen über alle Abbilder in einer Abbildgruppe anzeigen.

Vorabbereitstellen von Clientcomputern

Sie können WDS einsetzen, um physische Computer mit Computerkontoobjekten in AD DS-Servern zu verknüpfen. Dies wird als Vorabbereitstellung (pre-staging) des Clients bezeichnet. Vorab bereitgestellte Clients werden auch als *bekannte Computer* (known computer) bezeichnet. Sie können anschließend Eigenschaften für das Computerkonto konfigurieren, um die Installation des Clients zu steuern. So können Sie beispielsweise festlegen, welches Netzwerkstartprogramm und welche Antwortdatei für die unbeaufsichtigte Installation der Client erhält oder von welchem Server der Client das Netzwerkstartprogramm herunterlädt.

Sie führen keine Vorabbereitstellung für eine VHD durch, sondern für den Clientcomputer, der von dieser VHD startet.

Wenn Sie WDS im Rahmen der Abbildinstallation einsetzen, werden die Clientcomputer standardmäßig zu einer Domäne hinzugefügt. Sie können diese Funktion auf der Registerkarte *Client* im Eigenschaftendialogfeld des Servers deaktivieren.

Für die Vorabbereitstellung eines Clientcomputers, noch bevor Sie ein Abbild bereitstellen, können Sie das Tool WDSUTIL oder das Snap-In *Active Directory-Benutzer und -Computer* verwenden. Außerdem können Sie die Richtlinie zum automatischen Hinzufügen aktivieren. Wenn Sie diese Richtlinie aktivieren und die Installation eines unbekannten Clients genehmigen, wird die Installation fortgesetzt und in AD DS ein Computerkonto für diesen Client erstellt. Der WDSUTIL-Befehl zum Vorabbereitstellen eines Computers lautet `WDSUTIL /Add-Device /Device:<Name> /ID:<ID>`.

Wenn die Richtlinie zum automatischen Hinzufügen (auto-add policy) aktiviert ist, ist eine administrative Genehmigung erforderlich, bevor auf Clients, die nicht vorab bereitgestellt wurden, ein Abbild installiert werden darf. Sie aktivieren diese Richtlinie, indem Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen und eingeben: **WDSUTIL /Set-Server /AutoAddPolicy /Policy:AdminApproval**. Sie können die Richtlinie auch auf der Registerkarte *PXE-Antwort* im Eigenschaftendialogfeld eines Servers aktivieren.



Weitere Informationen Vorabbereitstellen von Clientcomputern mit dem Snap-In *Active Directory-Benutzer und -Computer*

Weitere Informationen, wie Sie Clientcomputer im Snap-In *Active Directory-Benutzer und -Computer* vorab bereitstellen, finden Sie unter *http://technet.microsoft.com/de-de/library/cc754289(WS.10).aspx*.

Die Vorabbereitstellung von Clients erhöht die Sicherheit. Sie können WDS so konfigurieren, dass es nur vorab bereitgestellten Clients antwortet. So ist sichergestellt, dass Clients, die nicht vorab bereitgestellt wurden, nicht über das Netzwerk starten können. Wenn Sie Clients vorab bereitstellen, können Sie folgende Elemente steuern:

- Name und Speicherort des Computerkontos in AD DS
- Welcher PXE-Server den Client bedient
- Welches Netzwerkstartprogramm der Client erhält
- Welches Startabbild ein Client empfängt und welche WDS-Clientantwortdatei für die unbeaufsichtigte Installation er benutzt

Die Vorabbereitstellung ermöglicht es, dasselbe Netzwerksegment von mehreren PXE-Servern bedienen zu lassen. Dazu werden die Server so eingeschränkt, dass sie nur jeweils einem bestimmten Teil der Clients antworten. Beachten Sie, dass die vorab bereitgestellten Clients in derselben Gesamtstruktur wie der WDS-Server liegen müssen.

Die Richtlinie zum automatischen Hinzufügen gilt nur, wenn der WDS-Server so eingestellt ist, dass er allen Clients antwortet, und wenn WDS kein vorab bereitgestelltes Computerkonto für einen startenden Computer findet. In allen anderen Fällen hat diese Richtlinie keine Auswirkung. Sie gilt nicht für Computer, die mit EFI (Extensible Firmware Interface) arbeiten.

Weitere Informationen Vorabbereitstellen von Clientcomputern

Weitere Informationen über die Vorabbereitstellung von Clientcomputern finden Sie unter *http://technet.microsoft.com/en-us/library/cc770832(WS.10).aspx.*

Übung Erstellen einer startfähigen VHD

In dieser Übung legen Sie in der Konsole *Computerverwaltung* eine VHD an. Dann fügen Sie die VHD zum Systemstartmenü hinzu, sodass Ihr Computer davon starten kann. Sie müssen die Übungen aus Lektion 1 durchgearbeitet haben, bevor Sie diese Übung beginnen.

Übung 1 Erstellen einer VHD

Gehen Sie folgendermaßen vor, um in der Computerverwaltung eine VHD anzulegen:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Legen Sie im Laufwerk *C:* einen Ordner namens *VHDs* an. Wenn es Ihnen lieber ist, können Sie auch ein externes USB-Festplattenlaufwerk verwenden. In diesem Fall müssen Sie den Laufwerkbuchstaben entsprechend anpassen. Stellen Sie aber sicher, dass das externe Laufwerk mit dem Dateisystem NTFS formatiert ist.
3. Klicken Sie im Startmenü mit der rechten Maustaste auf *Computer* und wählen Sie im Kontextmenü den Befehl *Verwalten*. Klicken Sie bei Bedarf auf *Ja*, um die Ausführung des Programms zu erlauben.
4. Wählen Sie den Zweig *Datenträgerverwaltung* aus.
5. Klicken Sie mit der rechten Maustaste auf *Datenträgerverwaltung* und wählen Sie den Befehl *Virtuelle Festplatte erstellen* (Abbildung 2.15).

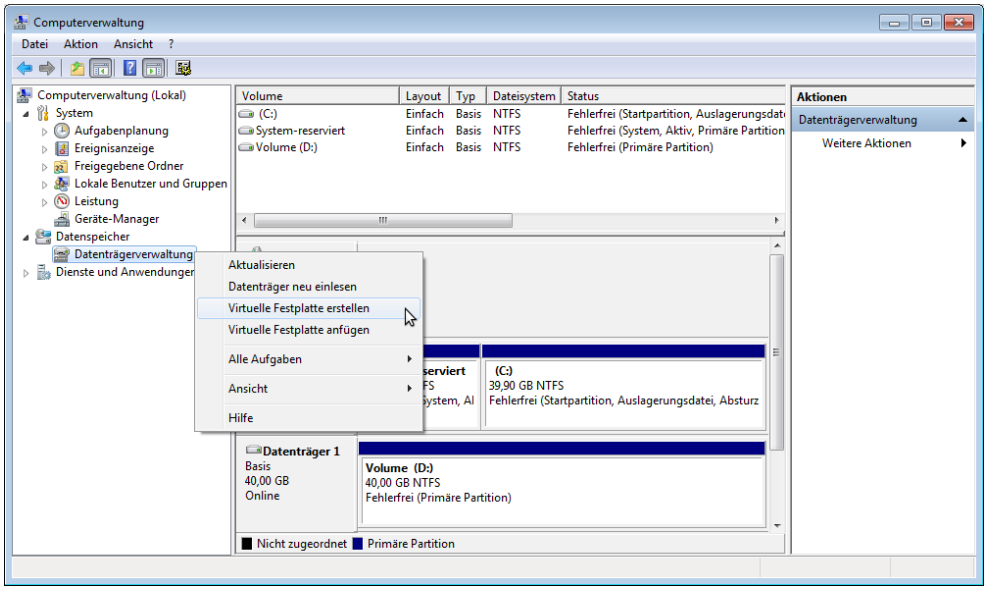


Abbildung 2.15 Erstellen einer VHD

6. Füllen Sie das Dialogfeld *Virtuelle Festplatte erstellen und anfügen* mit den Daten aus, die in Abbildung 2.16 gezeigt sind. Klicken Sie auf *OK*. Schließen Sie das Dialogfeld *Automatische Wiedergabe*, sofern es sich öffnet.

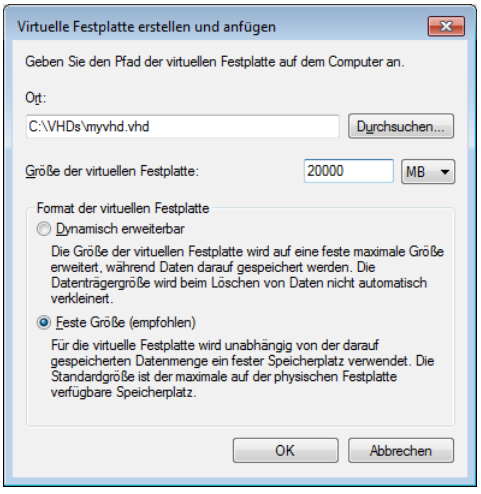

Virtuelle Festplatte erstellen und anfügen
Geben Sie den Pfad der virtuellen Festplatte auf dem Computer an.
Ort:
C:\VHDs\myvhd.vhd
Durchsuchen...
Größe der virtuellen Festplatte:
20000
MB
Format der virtuellen Festplatte
Dynamisch erweiterbar
Die Größe der virtuellen Festplatte wird auf eine feste maximale Größe erweitert, während Daten darauf gespeichert werden. Die Datenträgergröße wird beim Löschen von Daten nicht automatisch verkleinert.
Feste Größe (empfohlen)
Für die virtuelle Festplatte wird unabhängig von der darauf gespeicherten Datenmenge ein fester Speicherplatz verwendet. Die Standardgröße ist der maximale auf der physischen Festplatte verfügbare Speicherplatz.
OK
Abbrechen

Abbildung 2.16 Festlegen von Größe, Dateiname und Speicherort der VHD-Datei

7. Die VHD wird nun im Fensterabschnitt *Datenträgerverwaltung* aufgelistet (eventuell müssen Sie etwas warten). Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf das Symbol neben der Datenträgerbezeichnung der VHD und wählen Sie den Befehl *Datenträgerinitialisierung* (Abbildung 2.17).

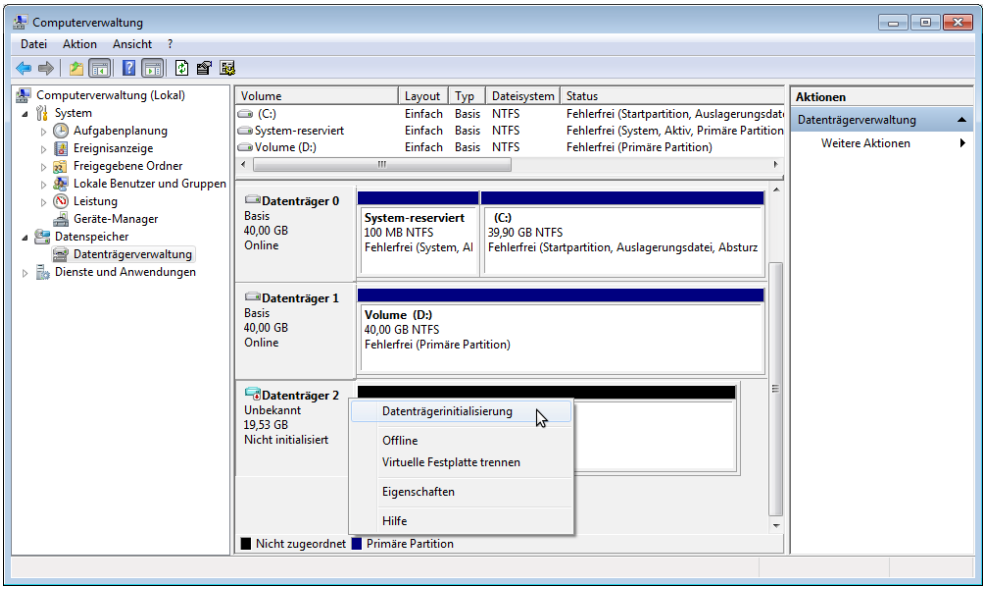


Abbildung 2.17 Initialisieren der VHD

8. Stellen Sie sicher, dass *MBR (Master Boot Record)* ausgewählt ist, und klicken Sie auf *OK*. Der Status des Datenträgers ändert sich auf *Online*.
9. Klicken Sie auf dem neu erstellten Datenträger mit der rechten Maustaste auf *Nicht zugeordnet* und wählen Sie den Befehl *Neues einfaches Volume*. Daraufhin wird der Assistent zum Erstellen neuer einfacher Volumes gestartet. Klicken Sie auf *Weiter*.
10. Klicken Sie auf *Weiter*, um die Standardeinstellung für die Volumegröße zu verwenden.
11. Wählen Sie auf der Seite *Laufwerkbuchstaben oder -pfad zuordnen* den Buchstaben *W* aus und klicken Sie auf *Weiter*.
12. Geben Sie dem Volume auf der Seite *Partition formatieren* eine Bezeichnung (zum Beispiel *MyVHD*, wie in Abbildung 2.18). Stellen Sie sicher, dass das Kontrollkästchen *Schnellformatierung durchführen* aktiviert ist. Klicken Sie auf *Weiter*.

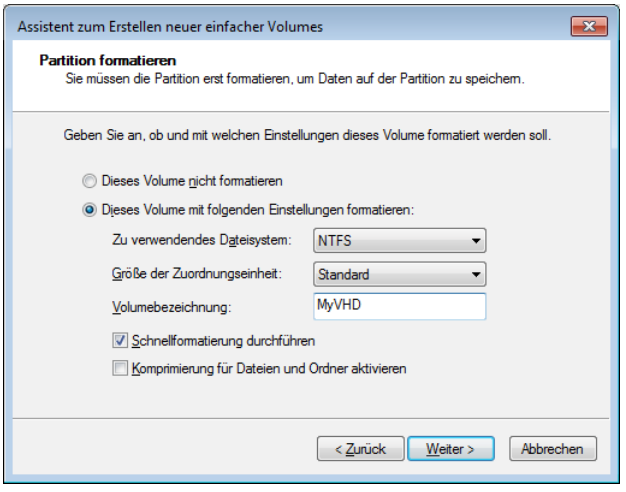

Assistent zum Erstellen neuer einfacher Volumes
Partition formatieren
Sie müssen die Partition erst formatieren, um Daten auf der Partition zu speichern.
Geben Sie an, ob und mit welchen Einstellungen dieses Volume formatiert werden soll.
Dieses Volume nicht formatieren
Dieses Volume mit folgenden Einstellungen formatieren:
Zu verwendendes Dateisystem:
NTFS
Größe der Zuordnungseinheit:
Standard
Volumebezeichnung:
MyVHD
Schnellformatierung durchführen
Komprimierung für Dateien und Ordner aktivieren
< Zurück
Weiter >
Abbrechen

Abbildung 2.18 Die Assistentenseite *Partition formatieren*

13. Klicken Sie auf *Fertig stellen*.

Übung 2 Hinzufügen einer VHD zum Systemstartmenü

Gehen Sie folgendermaßen vor, um die VHD, die Sie gerade erstellt haben, zum Systemstartmenü hinzuzufügen:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben Sie den Befehl **bcdedit /copy {current} /d "MyVHD"** ein. Wie in Abbildung 2.19 zu sehen, wird dabei die GUID des Ladeobjekts angezeigt. Diesen Wert tragen Sie in den nächsten Schritten dieser Übung für die Variable *<GUID>* ein. Die GUID auf Ihrem Computer unterscheidet sich von der in Abbildung 2.19.
3. Geben Sie den Befehl **bcdedit /set <*GUID*> device vhd=partition w:** ein.
4. Geben Sie **bcdedit /set <*GUID*> osdevice vhd=C:\vhds\myvhd.vhd** ein.
5. Zwingen Sie Windows 7, die HAL automatisch zu erkennen, indem Sie **bcdedit /set <*GUID*> detecthal on** ausführen.

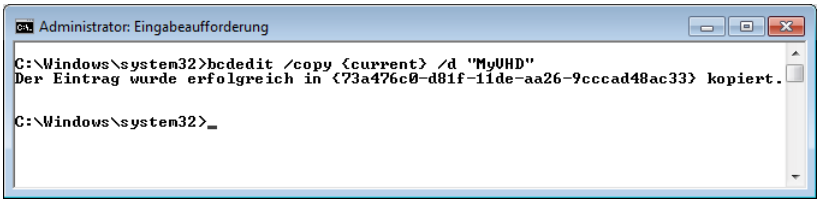


Abbildung 2.19 Ermitteln der GUID

6. Testen Sie, ob der Starteintrag richtig angelegt wurde, indem Sie **bcdedit /v** eingeben.
7. Kopieren Sie die WIM-Abbilddatei *Myimage.wim*, die Sie in Lektion 1 erstellt haben, in das startfähige Laufwerk *W:*.
8. Starten Sie den Computer neu. Prüfen Sie, ob Sie vom Gerät *MyVHD* starten können.

Zusammenfassung der Lektion

- Sie können das GUI-Tool *Datenträgerverwaltung* oder das Befehlszeilentool Diskpart verwenden, um auf einem Windows 7-Computer eine native VHD zu erstellen. Mit diesen Tools können Sie außerdem eine VHD anfügen, im Dateisystem bereitstellen, trennen und löschen.
- Mit dem Tool BCDEdit fügen Sie einen Starteintrag für eine VHD-Datei hinzu.
- Das Befehlszeilentool WIM2VHD erstellt aus WIM-Abbildern VHDs, die direkt in die OOBE-Phase starten.
- Mit dem Offline Virtual Machine Servicing Tool können Sie regelmäßige Updates für das Abbild auf startfähigen VHDs implementieren, die normalerweise offline sind. WDS stellt Tools zur Verfügung, mit denen Sie Abbilder auf Clientcomputern sowie auf virtuellen Computern und VHDs bereitstellen können, die online sind.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Verwalten von virtuellen Festplatten«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie wollen im Ordner *Windows7* einer externen USB-Festplatte mit dem Laufwerkbuchstaben *G:* eine 20 GByte große, native VHD mit dem Namen *Systemvhd* anlegen. Welchen Befehl verwenden Sie?
   A. **create vdisk file=g:\windows7\systemvhd maximum=20000**
   B. **create vdisk file=g:\windows7\systemvhd.vhd maximum=20000**
   C. **create vdisk file=g:\windows7\systemvhd.vhd maximum=20**
   D. **create vdisk file=g:\windows7\systemvhd maximum=20**

2. Sie haben mit dem Tool ImageX ein WIM-Systemabbild in einer VHD installiert und einen Starteintrag für diese VHD mit dem Tool BCDEdit hinzugefügt. Die startfähige VHD hat den Laufwerkbuchstaben *W:* bekommen. Die Variable *<GUID>* in den folgenden Befehlen wird durch die GUID der VHD ersetzt. Mit welchem Befehl prüfen Sie, ob Ihr Starteintrag richtig erstellt wurde?
   A. **bcdedit /set <*GUID*> detecthal on**
   B. **bcdedit /delete <*GUID*> /cleanup**
   C. **bcdedit /v**
   D. **bcdedit /copy {current} /d "Meine neue VHD"**
3. Sie wollen ein Installationsabbild zum Abbildspeicher auf einem WDS-Server hinzufügen. Die Quelle soll die Abbilddatei *Install.wim* im Ordner *C:/Myimages* sein. Welchen Befehl verwenden Sie?
   A. **WDSUTIL /Verbose /Progress /Replace-Image /Image:myimage.wim/ ImageType:Install /ImageGroup:<*MeineAbbildgruppe*> /ReplacementImage /ImageFile:C:\myimages/oldimage**
   B. **WDSUTIL /Set-Server /AutoAddPolicy /Policy:AdminApproval**
   C. **WDSUTIL /New-DiscoverImage /Image:myimage.wim /Architecture:x86 /DestinationImage /FilePath C:/myimages/install.wim**
   D. **WDSUTIL /Verbose /Progress /Add-Image /ImageFile:C:/myimages/install.wim /ImageType:Install**
4. Sie administrieren ein Netzwerk, in dem alle Clientcomputer unter Windows 7 Ultimate laufen. Sie haben auf allen Clients startfähige VHDs erstellt, damit im Fehlerfall eine Ausweichmöglichkeit zur Verfügung steht. Weil die VHDs normalerweise offline sind, erhalten die darin gespeicherten Abbilder aber nicht alle aktuellen Sicherheitsupdates. Sie wollen die Clients jeden Samstag um 23:30 automatisch von ihren VHDs starten und gerade so lange eingeschaltet lassen, bis sie die Updates von Ihrem WSUS-Server empfangen haben. Welches Tool verwenden Sie dafür?
   A. Offline Virtual Machine Servicing Tool
   B. SCVMM
   C. MMC-Snap-In *Windows-Bereitstellungsdienste*
   D. WDSUTIL

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Das Betriebssystem Windows 7 unterstützt native VHDs. Mit dem Tool BCDEdit können Sie eine VHD, die ein WIM-Abbild enthält, startfähig machen (nur in den Editionen Ultimate und Enterprise).
- Sie müssen das Windows AIK installieren, damit Sie WIM-Abbilddateien anlegen oder bereitstellen können. Zu den Windows AIK-Tools gehören Windows SIM, ImageX, Oscdimg, DISM, USMT und die Windows PE-Tools.
- Mit Diskpart und den Datenträgerverwaltungstools können Sie VHDs erstellen, anfügen und initialisieren. Mit dem Tool Sysprep können Sie ein Abbild verallgemeinern und computerspezifische Informationen entfernen.
- Die Windows-Bereitstellungsdienste stellen Tools zur Verfügung, um Abbilder für die Onlinebereitstellung zu erstellen und zu verwalten. Das Offline Virtual Machine Servicing Tool arbeitet mit SCVMM auf einem Windows-Server zusammen, um Updates auf Abbilder von Offline-VHDs anzuwenden.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Solution Accelerator**
- **Systemabbild**
- **Virtuelle Festplatte (Virtual Hard Disk, VHD)**
- **Windows Automated Installation Toolkit (Windows AIK)**
- **Windows Preinstallation Environment (Windows PE)**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie an, was Sie über das Konfigurieren von Systemabbildern gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Generieren eines Systemabbilds

Sie arbeiten als Enterpriseadministrator in einem sehr großen Softwareunternehmen. Sie wollen auf allen neuen Clientcomputern in Ihrer Organisation automatisch Windows 7 Ultimate installieren. Außerdem müssen Sie Benutzerdaten von Computern, die unter Windows Vista Ultimate laufen, auf Computer mit Windows 7 Ultimate übertragen. Ihr Unternehmen hat vor Kurzem ein Grafiktoolkit entwickelt, und Sie sollen ein Installationsabbild über das Internet verteilen, aus dem sich die Kunden eine Installations-DVD erstellen können. Beantworten Sie die folgenden Fragen:

1. Welche Art von Abbilddatei generieren Sie, um Windows 7 Ultimate zu installieren, und welches Tool verwenden Sie dafür?
2. Welche Art von Abbilddatei generieren Sie, um das Grafiktoolkit über das Internet zu verteilen, und welches Tool verwenden Sie dafür?
3. Welches Windows AIK-Tool benutzen Sie, um Benutzerdaten von Computern, die unter Windows Vista Ultimate laufen, auf Windows 7 Ultimate-Computer zu übertragen?

Übung mit Fallbeispiel 2: Arbeiten mit VHDs

Sie haben ein Testnetzwerk aufgebaut, um sich mit dem Betriebssystem Windows 7 vertraut zu machen. Das Netzwerk enthält zwei Clientcomputer. Der eine läuft unter Windows 7 Ultimate, der andere unter Windows 7 Home Premium. Beantworten Sie die folgenden Fragen:

1. Sie wollen auf Ihren Clientcomputern VHDs anlegen und WIM-Dateien erstellen, die jeweils den entsprechenden Computer als Referenzcomputer verwenden. Sie wollen die WIM-Referenzdateien auf beiden Clients in der VHD installieren und jeden Computer unter dem Betriebssystem starten, das auf der VHD gespeichert ist. Auf welchem Ihrer Clientcomputer funktioniert das?
2. Sie fügen drei weitere Clientcomputer zu Ihrem Testnetzwerk hinzu, auf denen Sie Windows 7 Ultimate installieren wollen. Sie nehmen den Windows 7 Ultimate-Computer aus Ihrem Netzwerk als Referenzcomputer. Welchen Sysprep-Befehl müssen Sie ausführen, bevor Sie eine WIM-Abbilddatei auf Ihrem Referenzcomputer aufzeichnen und das Abbild auf den neuen Clients installieren?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Verwenden von Windows SIM und Sysprep

In dieser Übung erstellen Sie eine Antwortdatei. Optional können Sie mithilfe dieser Antwortdatei Windows 7 auf einem Referenzcomputer installieren und dann mit dem Tool Sysprep die Installation verallgemeinern, bevor Sie eine Aufzeichnung davon in Form eines WIM-Abbilds anfertigen. Sie sollten dafür nicht den Computer *Canberra* verwenden, weil er für die anderen Lektionen in diesem Buch richtig konfiguriert sein muss; daher sind die Übungen 2 und 3 optional. Sie sollten sie durcharbeiten, wenn Sie einen anderen Clientcomputer haben, den Sie für diesen Zweck verwenden können.

- **Übung 1** Generieren Sie mit Windows SIM mehrere Antwortdateien. Schritt-für-Schritt-Anleitungen finden Sie unter *http://technet.microsoft.com/de-de/library/dd349348.aspx*.
- **Übung 2** Installieren Sie Windows 7 mithilfe einer der Antwortdateien, die Sie erstellt haben, auf einem Referenzcomputer. Auch zu diesem Vorgang finden Sie eine Anleitung unter der angegebenen URL.
- **Übung 3** Führen Sie `sysprep /generalize` aus, um hardwarespezifische Informationen vom Referenzcomputer zu entfernen und ein WIM-Abbild des Referenzcomputers zu generieren. Auch zu diesem Vorgang finden Sie eine Anleitung unter der URL, die in Übung 1 angegeben ist.

Arbeiten mit VHDs

Arbeiten Sie Übung 1 durch. Übung 2 ist optional.

- **Übung 1** Üben Sie, wie Sie VHDs anlegen, im Dateisystem bereitstellen, anfügen, trennen und löschen. Verwenden Sie dazu sowohl die Konsole *Datenträgerverwaltung* als auch Diskpart. Mit etwas Übung wird das ganz einfach. Machen Sie sich auch damit vertraut, wie Sie WIM-Abbilder auf VHDs installieren und mit BCDEdit startfähige VHDs erstellen.
- **Übung 2** Erstellen und konfigurieren Sie einen virtuellen Server, der unter Windows Server 2008 oder Windows Server 2008 R2 läuft. Installieren Sie das Offline Virtual Machine Servicing Tool und SCVMM. Erstellen Sie eine geplante Aufgabe, die Ihren Windows 7-Client von seiner startfähigen VHD startet.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

KAPITEL 3

Bereitstellen von Systemabbildern

Dieses Kapitel beschreibt die Verwaltung, Bearbeitung und Bereitstellung von Systemabbildern. Sie stellen ein Abbild bereit (deploy), wenn Sie es auf einem oder mehreren Zielcomputern installieren. Sie erfahren, wie Sie ein Systemabbild im Dateisystem bereitstellen, sodass es aktualisiert und bearbeitet werden kann, wie Sie die vorgenommenen Änderungen dann in das ursprüngliche Abbild übernehmen (commit) und wie Sie das Abbild auf mehrere – oft sehr viele – Clientcomputer verteilen. Im Bereich von Systemabbildern bedeutet *im Dateisystem bereitstellen* (mount), dass Sie ein Abbild in einen Ordner entpacken, sodass Sie Daten darüber erhalten und Features wie Treiber, Updates und Language Packs hinzufügen oder entfernen können.

Microsoft stellt etliche Tools für die Bearbeitung und Bereitstellung von Abbildern zur Verfügung. Einige davon sind speziell auf Windows 7-Abbilder zugeschnitten, andere haben einen breiteren Einsatzbereich. Manche Tools bearbeiten Abbilder, andere stellen sie bereit, und manche Tools erledigen beides. Es ist Ihre Aufgabe als Netzwerkadministrator, die besten Tools für Ihre aktuellen und künftigen Anforderungen auszuwählen und sie so zu konfigurieren, dass sie effizient funktionieren und das auch in Zukunft tun.

Wenn Ihre Benutzer mit Computern arbeiten, deren Betriebssysteme, Treiber und Anwendungen auf dem neusten Stand sind und die so gut wie möglich gegen Angriffe aus dem Internet (und Intranet) geschützt sind, sind die Benutzer zufriedener. Wenn Sie es schaffen, 1 oder auch 100 Computer schnell, effizient und fehlerfrei in Betrieb zu nehmen, ist Ihr Chef weniger unzufrieden. (Wir alle wissen natürlich, dass weder Benutzer noch Chefs jemals rundum zufrieden sind.)

In diesem Kapitel abgedeckte Prüfungsziele:

- Vorbereiten eines Systemabbilds für die Bereitstellung
- Bereitstellen eines Systemabbilds

Lektionen in diesem Kapitel:

- Lektion 1: Verwalten eines Systemabbilds vor der Bereitstellung 115
- Lektion 2: Bereitstellen von Abbildern 144

Bevor Sie beginnen

Um die Übungen in diesem Kapitel durchzuarbeiten, müssen Sie folgende Vorbereitungen getroffen haben:

- Sie haben Windows 7 auf einem eigenständigen Client-PC installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben. Sie brauchen Internetzugriff, um die Übungen durchzuführen.
- Sie haben alle Übungen in Kapitel 2, »Konfigurieren von Systemabbildern«, durchgearbeitet. Vor allem müssen Sie das Windows Automated Installation Kit (Windows AIK) installiert und ein Offlineabbild des Computers *Canberra* auf einer startfähigen virtuellen Festplatte bereitgestellt haben.

Praxistipp

Ian McLean

Alle Tools, die Sie für die Netzwerk- und Systemadministration einsetzen, haben einen eigenen Satz Features, der es Ihnen ermöglicht, bestimmte Aufgaben zu erledigen. Gelegentlich werden Administratoren gereizt oder verwirrt, wenn es Überschneidungen beim Funktionsumfang gibt. Zum Beispiel können Sie die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS) oder das Microsoft Deployment Toolkit 2010 (MDT) verwenden, um Windows 7-Abbilder auf Clientcomputern bereitzustellen. Sie können aber mit MDT 2010 eine Gruppe Konfigurationsaufgaben festlegen, die auf einem Computer ausgeführt werden sollen, nachdem ein Abbild über WDS darauf bereitgestellt wurde. Aber WDS ist nicht in der Lage, Konfigurationsaufgaben auf einem Client durchzuführen, nachdem das Abbild bereitgestellt wurde.

Sie verwenden ImageX, um das Abbild eines Windows 7-Computers anzufertigen, nachdem er unter Windows PE (Windows Preinstallation Environment) gestartet wurde. Und mit dem Tool DISM (Deployment Image Servicing and Management) bearbeiten Sie dieses Abbild, nachdem es erstellt worden ist. Sie können aber sowohl mit ImageX als auch mit DISM ein Abbild im Dateisystem bereitstellen, um offline damit zu arbeiten.

Die Frage ist also berechtigt, welches Tool Sie einsetzen sollten. Und in diesem Buch stellt sich besonders die Frage, welches Tool in der Prüfung behandelt wird. Einfache Antwort: Verwenden Sie das neuste Tool, wenn mehrere zur Wahl stehen. Beispielsweise gibt es ImageX schon längere Zeit, während DISM erst vor Kurzem eingeführt wurde. ImageX enthält allerdings in der neusten Version aus dem Windows AIK neue Features.

Die Prüfungen enthalten üblicherweise mehr Fragen über neue Features eines Betriebssystems und die neuen Tools, mit denen bestimmte Aufgaben unter dem neuen Betriebssystem ausgeführt werden. Features, die sich gegenüber der vorherigen Version des Betriebssystems nicht verändert haben, und Tools, die es schon länger gibt (auch wenn sie wichtig sind), werden nicht so ausführlich behandelt. Das ist eine simple Tatsache, und welche Schlüsse Sie daraus ziehen, bleibt Ihnen überlassen.

Aber auch wenn Sie die Prüfung ausklammern, stellt sich die Frage, welches Tool Sie als professioneller Administrator einsetzen. Die Entscheidung bleibt Ihnen überlassen. Mein Rat lautet: Wenn Sie DISM in letzter Zeit häufig eingesetzt haben und die DISM-Befehle im Halbschlaf eintippen können, sollten Sie dieses Tool verwenden, wenn mehrere zur

Wahl stehen. Andererseits bevorzuge ich ImageX, um ein Abbild im Dateisystem bereitzustellen. Die Befehle sind kürzer (wichtig, wenn Sie so langsam tippen wie ich), die Ausführung geschieht meinem Empfinden nach schneller, und wenn etwas schiefgeht, liefert ImageX normalerweise eine ausführlichere Erklärung. Das ist natürlich nur meine persönliche Meinung, Sie brauchen sich nicht an diese Empfehlung zu halten.

Als professioneller Administrator sollten Sie einfach auf Ihre Erfahrung vertrauen. Als Prüfungskandidat sollten Sie wissen, welche Funktionen alle Tools bieten, welche Fähigkeiten Alleinstellungsmerkmale eines Tools sind, welche Funktionen eines Tools nur im neuen Betriebssystem verfügbar sind oder bisher nicht möglich waren und für welche Aufgaben sich zwei oder mehr Tools gleich gut eignen.

Viel Glück.

Lektion 1: Verwalten eines Systemabbilds vor der Bereitstellung

Nachdem Sie ein Referenzabbild zum Bereitstellen auf anderen Computern angefertigt haben, stellt sich gelegentlich heraus, dass Sie es noch einmal ändern müssen. Vielleicht müssen Sie einen neuen Treiber hinzufügen, Einstellungen verändern oder zusätzliche Sprachen unterstützen. Selbst kleinere Änderungen, etwa das Aktivieren eines Features, das momentan im Abbild deaktiviert ist, können erheblichen Aufwand verursachen, wenn sie durchgeführt werden müssen, nachdem das Abbild bereits auf Hunderte von Computern verteilt wurde.

Im Allgemeinen ist der Aufwand geringer, wenn Sie die Änderungen vornehmen, ohne das Abbild bereitzustellen und dann neu aufzuzeichnen. Wenn Sie Sicherheitsupdates hinzufügen müssen, ist es sicherlich besser, die Sicherheitspatches offline einzuspielen – sonst stellen Sie ein unsicheres Abbild bereit. Falls Sie das Abbild offline bearbeiten, brauchen Sie nicht das Tool Sysprep auszuführen und somit auch nicht die Aktivierungsfrist zurückzusetzen. Und schließlich ist es sinnvoll, eine überarbeitete *Autounattend.xml*-Datei für die unbeaufsichtigte Installation oder eine zusätzliche *Unattend.xml*-Datei hinzuzufügen, die Aufgaben automatisiert, die nach der Installation durchgeführt werden, etwa um wichtige Anwendungen zu installieren. *Unattend.xml*-Dateien werden im Abschnitt »Befehlszeilenoptionen für unbeaufsichtigte Bearbeitung«, weiter unten in diesem Kapitel beschrieben.

Diese Lektion beschreibt, wie Sie mithilfe von Windows AIK-Tools wie ImageX und DISM ein Systemabbild im Dateisystem bereitstellen und mit DISM das Abbild verwalten, Pakete einfügen, Updates einspielen, Features aktivieren oder deaktivieren, internationale Einstellungen verwalten, Language Packs verwalten und Antwortdateien für unbeaufsichtigte Installationen verknüpfen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Bereitstellen eines Offlineabbilds im Dateisystem, um es zu bearbeiten
- Verwalten und Bearbeiten des Abbilds mit DISM
- Verknüpfen einer oder mehrerer Antwortdateien mit dem Abbild
- Übernehmen von Änderungen in das Abbild und Aufheben der Bereitstellung im Dateisystem

Veranschlagte Zeit für diese Lektion: 50 Minuten

Verwenden der WIM-Befehle von DISM und Bereitstellen eines Abbilds im Dateisystem

Kapitel 2 hat das Windows 7-Befehlszeilentool DISM vorgestellt. Mit DISM können Sie Offlineabbilder bearbeiten, WIM-Dateien (Windows Imaging) im Dateisystem bereitstellen oder die Bereitstellung im Dateisystem aufheben und Windows PE-Startabbilder anpassen Das Tool DISM ersetzt gleich mehrere Tools aus den Vorgängerversionen des Windows AIK, darunter den Paketmanager (*Pkgmgr.exe*), das Konfigurationstool für internationale Einstellungen (*Intlcfg.exe*) und das Windows PE-Befehlszeilentool (*PEimg.exe*).

Microsoft hat DISM für die Aufgabe entworfen, WIM-Abbilder zu verwalten. DISM ist außerdem abwärtskompatibel zu Windows Vista-Tools wie *Pkgmgr.exe*, *Intlcfg.exe* und *PEimg.exe*, sodass Skripts, die Sie für Windows Vista entwickelt und getestet haben, unverändert auch in Windows 7 funktionieren sollten.



Hinweis Abwärtskompatibilität

Sie können das Windows AIK für Windows 7 (inklusive DISM) auf Windows Vista SP1 installieren. Wenn Sie Windows 7- und Windows Server 2008 R2-Abbilder unter Windows Vista verwalten, erhalten Sie dank dieser Abwärtskompatibilität den vollständigen Funktionsumfang. DISM beherrscht auch den Umgang mit Windows Vista SP1- und Windows Server 2008-Abbildern, allerdings nur mit eingeschränkten Funktionen. Sie können für Windows Vista SP1-Abbilder alle Features von DISM verwenden, die schon in *Pkgmgr.exe*, *Intlcfg.exe* oder *PEimg.exe* verfügbar waren. Allerdings erhalten Sie eine Fehlermeldung, wenn Sie eine Befehlszeilenoption verwenden, die für ein Windows Vista-Abbild nicht unterstützt wird.

Kapitel 2 hat auch das Tool ImageX eingeführt, mit dem Sie eine WIM-Abbilddatei erstellen. In den meisten Fällen haben Sie die Wahl, ob Sie DISM oder ImageX einsetzen, um WIM-Dateien im Dateisystem bereitzustellen. DISM ist das empfohlene Windows AIK-Tool zum Verwalten und Bearbeiten von Offlineabbildern. Sie können damit Betriebssystemupdates, Pakete und Treiber in einem Offlinesystemabbild installieren und konfigurieren. Mit DISM können Sie Windows PE-Abbilder offline ändern und die Einstellungen für Sprache, Gebietsschema, Schriftart und Eingabe eines Windows-Abbilds konfigurieren.

Welche Befehle DISM für die Abbildverwaltung anbietet, hängt davon ab, welche Art Abbild Sie verwalten. Sie greifen auf DISM zu, indem Sie im Startmenü *Alle Programme* und dann *Microsoft Windows AIK* wählen, mit der rechten Maustaste auf *Eingabeaufforderung für Bereitstellungstools* klicken und im Kontextmenü den Befehl *Als Administrator ausführen* wählen. Unter Umständen müssen Sie auf *Ja* klicken, um die Ausführung des Programms zu erlauben. Geben Sie im Fenster *Eingabeaufforderung für Bereitstellungstools* den Befehl **dism** ein, um sich eine Liste aller DISM-Befehle anzeigen zu lassen. Abbildung 3.1 zeigt Befehle für die Verwaltung von WIM-Abbildern.

Beispielsweise liefert der folgende Befehl Informationen über *Myimage.wim*, die WIM-Datei, die Sie in Kapitel 2 erstellt und auf einer startfähigen VHD mit dem Laufwerkbuchstaben *W:* installiert haben:

```
dism /get-wiminfo /wimfile:w:\myimage.wim
```

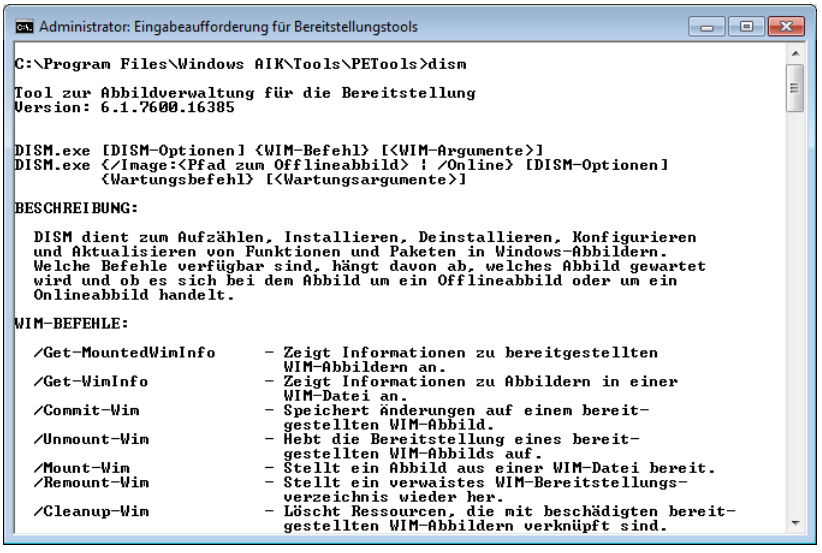

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>dism
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
DISM.exe [DISM-Optionen] {WIM-Befehl} [<WIM-Argumente>]
DISM.exe {/Image:<Pfad zum Offlineabbild> | /Online} [DISM-Optionen]
{Wartungsbefehl} [<Wartungsargumente>]
BESCHREIBUNG:
DISM dient zum Aufzählen, Installieren, Deinstallieren, Konfigurieren
und Aktualisieren von Funktionen und Paketen in Windows-Abbildern.
Welche Befehle verfügbar sind, hängt davon ab, welches Abbild gewartet
wird und ob es sich bei dem Abbild um ein Offlineabbild oder um ein
Onlineabbild handelt.
WIM-BEFEHLE:
/Get-MountedWimInfo - Zeigt Informationen zu bereitgestellten WIM-Abbildern an.
/Get-WimInfo - Zeigt Informationen zu Abbildern in einer WIM-Datei an.
/Commit-Wim - Speichert Änderungen auf einem bereitgestellten WIM-Abbild.
/Unmount-Wim - Hebt die Bereitstellung eines bereitgestellten WIM-Abbilds auf.
/Mount-Wim - Stellt ein Abbild aus einer WIM-Datei bereit.
/Remount-Wim - Stellt ein verwaistes WIM-Bereitstellungsverzeichnis wieder her.
/Cleanup-Wim - Löscht Ressourcen, die mit beschädigten bereitgestellten WIM-Abbildern verknüpft sind.

Abbildung 3.1 DISM-Befehle zum Verwalten von WIM-Abbildern

Die Ausgabe dieses Befehls sehen Sie in Abbildung 3.2. Falls dieser Befehl das Abbild nicht findet, müssen Sie die Computerverwaltung öffnen und die VHD anfügen. Es handelt sich um die Datei *Myvhd.vhd* im Ordner *VHDs*. Falls Sie keine VHD angelegt haben, können Sie auch die Version der WIM-Datei aus dem Ordner *D:\Images* verwenden (oder dem Ordner, den Sie in der Übung von Kapitel 2 verwendet haben). Ist die Datei *Myimages.wim* überhaupt nicht vorhanden, können Sie stattdessen die Datei *Install.wim* von Ihrer Installations-DVD in *D:\Images* kopieren und sie verwenden.

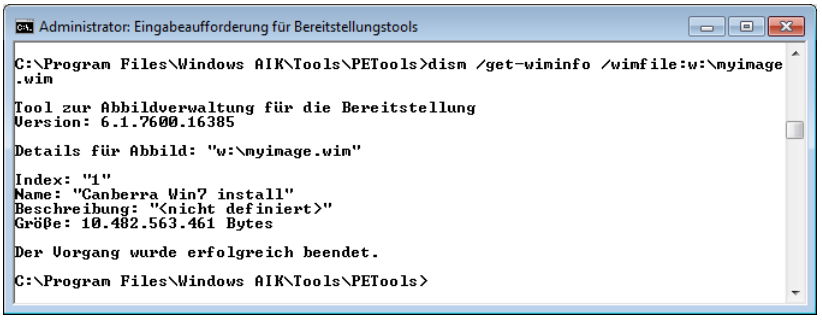


Abbildung 3.2 Verwenden der Optionen `/Get-WimInfo` und `/Wimfile`

Brauchen Sie ausführlichere Informationen über das Abbild, können Sie das Tool ImageX verwenden:

```
imagex /info w:\myimage.wim
```

Abbildung 3.3 zeigt einen Ausschnitt aus der Ausgabe dieses Befehls. Die Datei enthält nur ein Abbild, das den Index 1 hat. (Wenn Sie das *Install.wim*-Abbild verwenden wollen, müssen Sie die Indexnummer für das Windows 7 Ultimate-Abbild ermitteln, gewöhnlich ist es 5.)

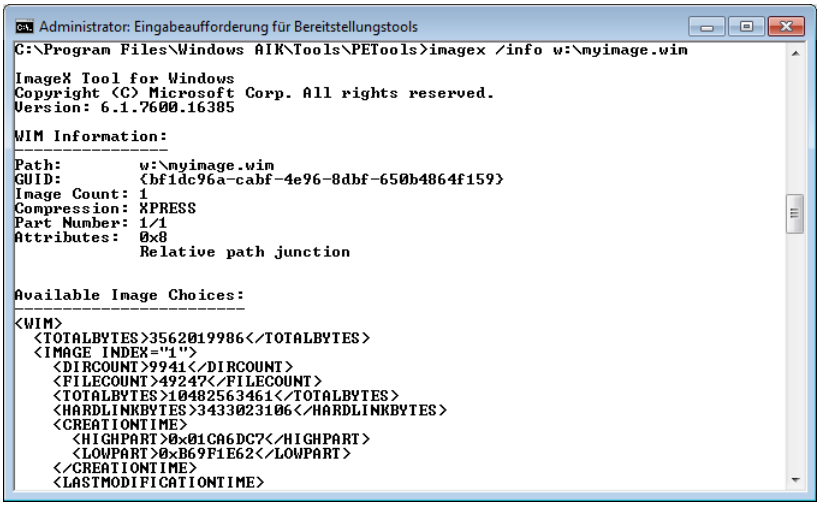


Abbildung 3.3 Ausführliche Informationen über ein WIM-Abbild

Bereitstellen von WIM-Abbildern im Dateisystem

Um ein Abbild bearbeiten zu können, müssen Sie es erst im Dateisystem bereitstellen (mount). Geben Sie in der erhöhten Eingabeaufforderung für Bereitstellungstools den folgenden Befehl ein, um das Abbild *W:\Myimage.wim* im Ordner *C:\MountedImages* bereitzustellen:

```
dism /mount-wim /wimfile:w:\myimage.wim /index:1 /mountdir:c:\mountedimages
```

Das Flag `/index` in diesem Befehl gibt an, welches Abbild Sie im Dateisystem bereitstellen. Innerhalb derselben WIM-Datei können sich mehrere Abbilder befinden (beispielsweise unterschiedliche Editionen von Windows 7).

Sie können das Flag `/readonly` zu diesem Befehl hinzufügen, wenn Sie das Abbild schreibgeschützt bereitstellen wollen. Stattdessen können Sie auch in derselben Eingabeaufforderung das Tool ImageX verwenden. Hier lautet der entsprechende Befehl:

```
imagex /mountrw w:\myimage.wim 1 c:\mountedimages
```

Wollen Sie beide Befehle ausprobieren, müssen Sie für den zweiten Befehl einen anderen Zielordner anlegen und verwenden (zum Beispiel *C:\Othermount*). Der Zielordner darf vor der Bereitstellung keine Dateien enthalten. Stattdessen können Sie auch das bereitgestellte Abbild im Ordner *C:\MountedImages* löschen und es erneuern. Zum Löschen eines bereitgestellten Abbilds können Sie nicht den Windows-Explorer verwenden, Sie müssen den folgenden ImageX-Befehl ausführen, um die Bereitstellung des Abbilds im Dateisystem aufzuheben:

```
imagex /unmount c:\mountedimages
```

Auch mit DISM können Sie die Bereitstellung einer WIM-Datei im Dateisystem aufheben. Der entsprechende Befehl sieht so aus:

```
dism /unmount-wim c:\mountedimages
```

Diese Befehle verwenden Sie in der Übung weiter unten in dieser Lektion.



Hinweis **Bereitstellen der Datei *Install.wim* von der Installations-DVD**

Sie können die Datei *Install.wim* von der Installations-DVD im Dateisystem bereitstellen. Dabei erhalten Sie aber nur ein schreibgeschütztes Abbild, deshalb müssen Sie das Flag `/readonly` angeben, wenn Sie den DISM-Befehl ausführen. Wenn Sie ein Abbild bereitstellen wollen, das Sie auch ändern können, müssen Sie *Install.wim* erst auf einen beschreibbaren Datenträger kopieren und sicherstellen, dass das Dateiattribut *Schreibgeschützt* nicht gesetzt ist.

Ermitteln von Informationen über bereitgestellte WIM-Abbilder

Der folgende Befehl liefert Informationen über alle WIM-Dateien, die im Dateisystem Ihres Computers bereitgestellt sind:

```
dism /get-mountedwiminfo
```

Die Ausgabe dieses Befehls sehen Sie in Abbildung 3.4.

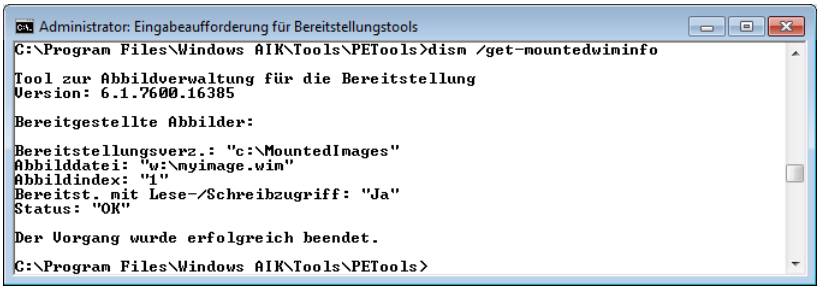


Abbildung 3.4 Im Dateisystem des Computers bereitgestellte WIM-Dateien

Wenn Sie mit den Dateien aus einem bereitgestellten Abbild arbeiten, ist es sinnvoll, ein temporäres Verzeichnis anzulegen, in dem Sie diese Dateien ablegen. Zuerst müssen Sie einen Ordner für die Dateien anlegen (beispielsweise *C:\Arbeitsdateien*). Geben Sie dann den folgenden Befehl ein:

```
dism /image:c:\mountedimages /scratchdir:c:\arbeitsdateien
```

Wenn Sie ein Abbild im Lese-/Schreibmodus bereitgestellt haben, können Sie darin vorhandene Dateien erweitern und Aktualisierungen sowie Anwendungen und Treiber hinzufügen. Sie können die Edition festlegen, internationale Einstellungen konfigurieren und Language Packs hinzufügen. Diese Vorgänge sind weiter unten in dieser Lektion beschrieben. Sie können alle Änderungen, die Sie am Offlineabbild vorgenommen haben, speichern oder *übernehmen* (commit), indem Sie folgenden Befehl ausführen:

```
dism /commit-wim /mountdir:c:\mountedimages
```

Es kann einige Zeit dauern, bis dieser Befehl abgeschlossen ist. In diesem Beispiel werden alle Änderungen, die Sie an dem Abbild, das in *C:\MountedImages* bereitgestellt ist, vorgenommen haben, im Quellabbild *W:\Myimage.wim* gespeichert. Der Befehl hebt die Bereitstellung des Abbilds im Dateisystem nicht auf. Sie haben daher die Möglichkeit, das Abbild noch weiter zu bearbeiten und danach erneut zu speichern. Abbildung 3.5 zeigt die Ausgabe dieses Befehls.

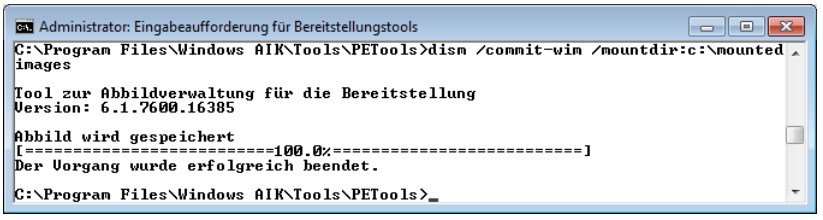


Abbildung 3.5 Speichern eines bereitgestellten WIM-Abbilds, das verändert wurde

Es kann vorkommen, dass Dateien in einem bereitgestellten WIM-Abbild beschädigt werden. In diesem Fall wollen Sie nicht, dass diese Dateien in das Quellabbild zurückgeschrieben werden. Außerdem kann es passieren, dass ein bereitgestelltes Abbild »verwaist«, weil sich die Verzeichnisstruktur ändert. Der folgende Befehl entfernt beschädigte Dateien aus allen bereitgestellten Abbildern des Computers:

```
dism /cleanup-wim
```

Abbildung 3.6 zeigt, wie alle beschreibbaren Volumes nach beschädigten Dateien durchsucht werden.

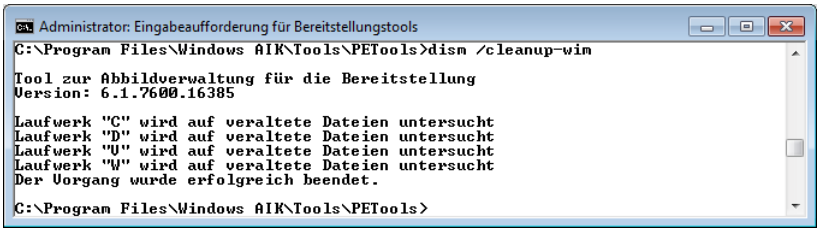

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>dism /cleanup-wim
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
Laufwerk "C" wird auf veraltete Dateien untersucht
Laufwerk "D" wird auf veraltete Dateien untersucht
Laufwerk "U" wird auf veraltete Dateien untersucht
Laufwerk "W" wird auf veraltete Dateien untersucht
Der Vorgang wurde erfolgreich beendet.
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.6 Suchen nach beschädigten Dateien

Und mit dem folgenden Befehl können Sie verwaiste Abbilder ermitteln und neu im Dateisystem bereitstellen:

```
dism /remount-wim /mountdir:c:\mountedimages
```



Prüfungstipp

Prägen Sie sich den Unterschied ein zwischen `/cleanup-wim`, das beschädigte Dateien entfernt, `/remount-wim`, das verwaiste Abbilder ermittelt und neu im Dateisystem bereitstellt, und `/cleanup-image`. Das letzte Argument wird meist mit `/RevertPendingActions` kombiniert, um eine Systemwiederherstellung zu versuchen, nachdem ein Fehler beim Systemstart aufgetreten ist. Diese Operation macht alle ausstehenden Aktionen aus vorherigen Bearbeitungsvorgängen rückgängig, weil diese Aktionen den Systemstartfehler möglicherweise verursachen. Beachten Sie, dass `/RevertPendingActions` nicht auf einem laufenden Betriebssystem oder bei einem Windows PE- oder Windows RE-Abbild unterstützt wird.

Arbeiten mit einem Onlineabbild

Es ist nicht nur möglich, ein Offlineabbild im Dateisystem bereitzustellen und zu bearbeiten, sondern auch, mit dem Betriebssystemabbild zu arbeiten, das momentan online ist. Zum Beispiel listet der folgende Befehl alle Out-of-Box-Treiber (Standardtreiber) auf, die momentan installiert sind:

```
dism /online /get-drivers
```

Abbildung 3.7 zeigt einen Ausschnitt aus der Ausgabe dieses Befehls. Brauchen Sie eine Liste aller Treiber, also nicht nur der Out-of-Box-Treiber, können Sie `/all` an diesen Befehl anhängen.

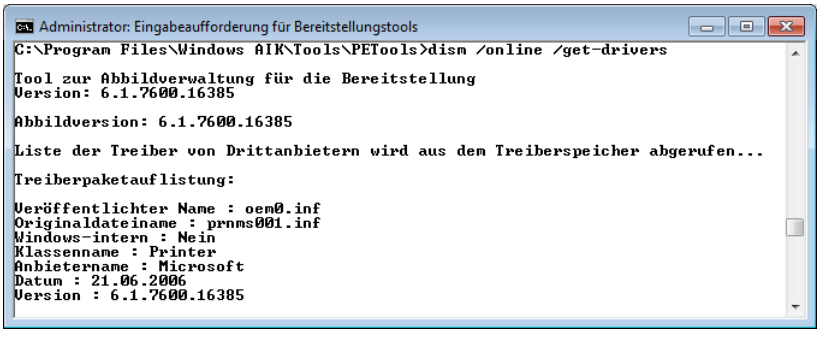


Abbildung 3.7 Auflisten der Treiber im Onlinesystemabbild

Meist rufen Sie zu einem Onlineabbild nur Informationen ab, ohne es zu erweitern oder zu verändern. So können Sie einen Befehl wie `dism /online /get-currentedition`, der die Edition des Betriebssystems ermittelt, in einer Batchdatei aufrufen, in der es von der Windows 7-Edition abhängen soll, welche Aktion ausgeführt wird. Tabelle 3.1 listet auf, welche Argumente Sie zusammen mit der Option `/online` verwenden können.

Tabelle 3.1 Argumente, die für Onlineabbilder benutzt werden können

Argument	Beschreibung
`/Get-CurrentEdition`	Zeigt die Edition des Onlineabbilds an.
`/Get-StagedEditions`	Zeigt eine Liste der Microsoft Windows-Editionen an, die aus einem Abbild entfernt werden können.
`/Get-TargetEditions`	Zeigt eine Liste der Windows-Editionen an, auf die das Onlineabbild aktualisiert werden kann.
`/Get-DriverInfo`	Zeigt Informationen über einen bestimmten Treiber an.
`/Get-Drivers`	Zeigt Informationen über alle Out-of-Box-Treiber an.
`/Get-Intl`	Zeigt Informationen über die internationalen Einstellungen und Sprachen an.
`/Get-Packages`	Zeigt Informationen über alle Pakete im Onlineabbild an.
`/Get-PackageInfo`	Zeigt Informationen über ein bestimmtes Paket an.
`/Get-Features`	Zeigt Informationen über alle Features im Onlineabbild an.
`/Get-FeatureInfo`	Zeigt Informationen über ein bestimmtes Feature an.

Alle Argumente, die online benutzt werden können, stehen auch offline zur Verfügung, wenn Sie mit `/image` ein im Dateisystem bereitgestelltes WIM-Abbild angeben. Zum Beispiel listet der folgende Befehl alle Treiber aus dem Abbild auf, das im Ordner *C:\MountedImages* bereitgestellt ist:

```
dism /image:c:\mountedimages /get-drivers /all
```

Tabelle 3.2 listet die Argumente zum Abrufen von Informationen auf, die Sie nur bei einem offline bereitgestellten Abbild, aber nicht beim Onlineabbild verwenden können.

Tabelle 3.2 Argumente, die nur bei Offlineabbildern zur Verfügung stehen

Argument	Beschreibung
`/Get-AppPatchInfo`	Zeigt Informationen über installierte Windows Installer-Patchdateien (MSP-Patches) an.
`/Get-AppPatches`	Zeigt Informationen über alle angewendeten MSP-Patches für alle installierten Anwendungen an.
`/Get-AppInfo`	Zeigt Informationen über eine bestimmte installierte Windows Installer-Anwendung (MSI-Anwendung) an.
`/Get-Apps`	Zeigt Informationen über alle installierten MSI-Anwendungen an.

Warten von Treibern, Anwendungen, Patches, Paketen und Features

Mithilfe der Treiberwartungsbefehle können Sie ein offline bereitgestelltes Abbild bearbeiten, um darin Treiber, die im *.inf*-Dateiformat vorliegen, hinzuzufügen und zu entfernen. Sie geben dabei entweder ein Verzeichnis an, in dem die *.inf*-Dateien der Treiber liegen, oder wählen einen Treiber durch Angabe des Namens der *.inf*-Datei aus.

Bei einem online laufenden Betriebssystem können Sie nur die Treiber auflisten lassen und Informationen über die Treiber abrufen. Die Befehle und Optionen zum Auflisten von Treibern und Abrufen von Treiberinformationen wurden im vorherigen Abschnitt dieser Lektion beschrieben. DISM kann ausschließlich Treiber verwalten, die als *.inf*-Datei vorliegen. MSI- (Windows Installer) und andere Treiberpakettypen (etwa *.exe*-Dateien) werden nicht unterstützt.

Für ein Offlineabbild stehen folgende Treiberwartungsoptionen zur Verfügung:

```
dism /image:<Pfad_zum_Abbildverzeichnis> [/get-drivers | /get-driverinfo | /add-driver |
/remove-driver]
```

Wollen Sie beispielsweise den Treiber *Mydriver.inf* hinzufügen, den Sie heruntergeladen und im Ordner *C:\Newdrivers* gespeichert haben, verwenden Sie folgenden Befehl:

```
dism /image:c:\mountedimages /add-driver:c:\newdrivers\mydriver.inf
```

Abbildung 3.8 zeigt die Ausgabe dieses Befehls.

Wenn Sie einen neuen Treiber hinzufügen, sollten Sie ihn an einem praktischen Speicherort ablegen. Dann können Sie Dateinamen und Pfad direkt hinter dem Argument `Add-Drivers` angeben und brauchen nicht das Argument `/driver` zu verwenden. Wollen Sie dagegen mehrere Treiber hinzufügen, die sich im selben Ordner befinden, verwenden Sie folgenden Befehl:

```
dism /image:c:\mountedimages /add-driver /driver:c:\newdrivers
```

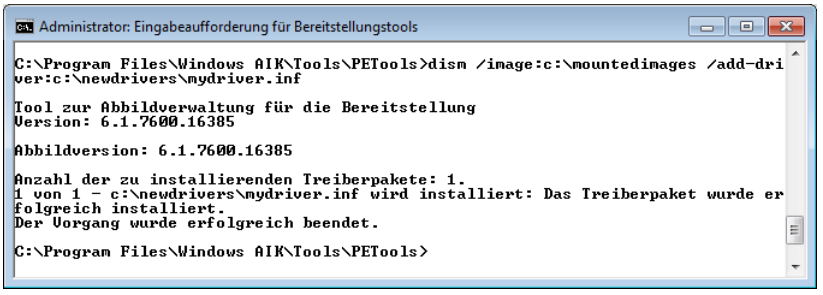

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mountedimages /add-dri
ver:c:\newdrivers\mydriver.inf
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
Abbildversion: 6.1.7600.16385
Anzahl der zu installierenden Treiberpakete: 1.
1 von 1 - c:\newdrivers\mydriver.inf wird installiert: Das Treiberpaket wurde er
folgreich installiert.
Der Vorgang wurde erfolgreich beendet.
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.8 Hinzufügen eines Treibers zu einem Abbild

Wenn Sie alle Treiber hinzufügen wollen, die in mehreren Ordnern vorliegen, können Sie das Argument `/driver` so oft wie nötig angeben. Hier ein Beispiel:

```
dism /image:c:\mountedimages /add-driver /driver:c:\printdrivers /driver:d\nicdrivers
```

Und wenn Sie alle Treiber aus einem Ordner und seinen Unterordnern hinzufügen wollen, können Sie das Argument `/recurse` verwenden (Abbildung 3.9):

```
dism /image:c:\mountedimages /add-driver /driver:c:\newdrivers /recurse
```

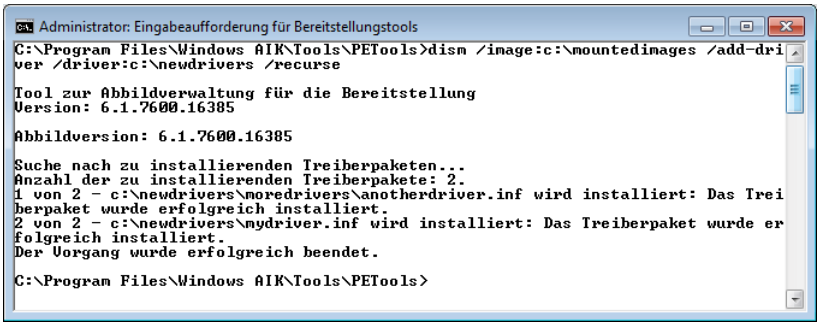

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mountedimages /add-dri
ver /driver:c:\newdrivers /recurse
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
Abbildversion: 6.1.7600.16385
Suche nach zu installierenden Treiberpaketen...
Anzahl der zu installierenden Treiberpakete: 2.
1 von 2 - c:\newdrivers\moredrivers\anotherdriver.inf wird installiert: Das Trei
berpaket wurde erfolgreich installiert.
2 von 2 - c:\newdrivers\mydriver.inf wird installiert: Das Treiberpaket wurde er
folgreich installiert.
Der Vorgang wurde erfolgreich beendet.
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.9 Verwenden der Option `/recurse`

Auf Computern mit einer x64-Version von Windows 7 müssen Treiber eine digitale Signatur haben. Gelegentlich ist es allerdings nötig, für Testzwecke einen unsignierten Treiber zu installieren. In einem solchen Fall können Sie das Argument `/forceunsigned` angeben, um diese Anforderung außer Kraft zu setzen.

Mit dem Argument `/remove-drivers` löschen Sie die Treiber anderer Hersteller aus einem Offlineabbild. Standardtreiber können Sie mit dem Befehl `dism` nicht entfernen. Wenn Sie Treiber anderer Hersteller hinzufügen, heißen sie *oem0.inf*, *oem1.inf* und so weiter. Sie müssen den veröffentlichten Namen angeben, aber glücklicherweise listet das Argument `/get-drivers` sowohl den veröffentlichten als auch den ursprünglichen Namen auf. Wenn Sie viele Treiber anderer Hersteller installiert haben und Schwierigkeiten haben, den neuen Namen des Treibers herauszufinden, den Sie löschen wollen, können Sie die Ausgabe eines `dism`-Befehls, der mit dem Argument `/get-drivers` aufgerufen wird, in eine Textdatei umleiten und diese Datei nach dem ursprünglichen Namen durchsuchen. Sobald Sie den veröffentlichten Namen des Treibers herausgefunden haben, beispielsweise *oem10.inf*, können Sie ihn mit dem folgenden Befehl löschen:

```
dism /image:c:\mountedimages /remove-driver /driver:oem10.inf
```

Warten von Anwendungen und Anwendungspatches

Indem Sie die Befehlszeilenoptionen für die Anwendungswartung auf ein Offlineabbild anwenden, können Sie prüfen, ob Windows Installer-Anwendungspatches eingespielt werden können, und aus dem Offlineabbild Informationen über die installierten Windows Installer-Anwendungen (*.msi*-Dateien) und Anwendungspatches (*.msp*-Dateien) abrufen.

Keinen der Anwendungswartungsbefehle können Sie auf Onlineabbilder anwenden. Solange ein Abbild online ist, kann es allerdings Updates von WSUS (Windows Server Update Services), Microsoft Update oder anderen Quellen erhalten. Wenn Sie ein großes Unternehmensnetzwerk verwalten, sollten Sie sich das Offline Virtual Machine Servicing Tool und den System Center Virtual Machine Manager genauer ansehen und prüfen, ob sie sich für Ihre Umgebung eignen; diese Tools wurden in Kapitel 2 vorgestellt.

DISM stellt folgende Optionen zur Verfügung, um Windows Installer-Anwendungen (*.msi*) und *.msp*-Anwendungspatches aufzulisten und zu prüfen, ob ein Anwendungspatch auf ein Offlinesystemabbild angewendet werden kann:

```
dism /image:<Pfad_zum_Verzeichnis> [/check-apppatch | /get-apppatchinfo: |
/get-apppatches | /get-appinfo | /get-apps]
```

Wenn Sie Anwendungen und Patches verwalten, sollten Sie im ersten Schritt feststellen, welche Anwendungspatches und Anwendungen vorhanden sind und welche sich auf das Abbild anwenden lassen. Wurde ein Abbild beispielsweise direkt aus einer *Install.wim*-Datei bereitgestellt, die vom Installationsmedium kopiert wurde, gibt es wahrscheinlich keine anwendbaren Patches oder Anwendungen. Mit einem Befehl wie dem folgenden rufen Sie Informationen über Anwendungspatches (*.msi*-Dateien) ab, die auf ein bereitgestelltes Abbild angewendet werden können:

```
dism /image:c:\mountedimages /get-apppatches
```

Wenn Sie die Produktcode-GUID (Globally Unique Identifier) einer Windows Installer-Anwendung wissen, können Sie das Argument `/productcode` verwenden, um alle Anwendungspatches in der angegebenen Anwendung aufzulisten. Dazu verwenden Sie den folgenden Befehl:

```
dism /image:c:\mountedimages /get-apppatches /productcode:<{GUID}>
```

Mit dem Argument `/check-apppatch` erhalten Sie Informationen über bestimmte *.msp*-Patches, die auf das Offlineabbild angewendet werden können. Geben Sie dabei mit `/patchlocation` den Pfad zur *.msp*-Patchdatei an. Mit `/patchlocation` können Sie mehrere Patchdateien im selben Befehl angeben. Zum Beispiel zeigt der folgende Befehl Informationen über die zwei Patchdateien *30880d0.msp* und *8c82a.msp* (beide in *C:\Windows\Installer*) im bereitgestellten Abbild an:

```
dism /image:c:\mountedimages /check-apppatch /patchlocation:c:\windows\installer\
30880d0.msp /patchlocation:c:\windows\installer\8c82a.msp
```

Brauchen Sie ausführliche Informationen über alle installierten MSP-Patches, die sich auf das Offlineabbild anwenden lassen, können Sie folgenden Befehl eingeben:

```
dism /image:c:\mountedimages /get-apppatchinfo
```

Schnelltest

- Sie wollen alle Treiber aus dem Ordner *C:\Orinsnewdrivers* und seinen Unterordnern auf das in *D:\Orinsimage* bereitgestellte Offlineabbild anwenden. Welchen Befehl benutzen Sie?

Antwort zum Schnelltest

- `dism /image:d:\orinsimage /add-driver /driver:d:\orinsimage /recurse`

Mit dem Argument `/get-apppatches`, das bereits weiter oben in diesem Abschnitt beschrieben wurde, finden Sie die Patchcode-GUID und die Produktcode-GUID für einen bestimmten Patch heraus. Sie können auch das Argument `/get-apps` verwenden, um alle Produktcode-GUIDs für eine installierte Windows Installer-Anwendung aufzulisten. Die Informationen, die beim Aufruf von `/get-apppatchinfo` zurückgegeben werden, können Sie entweder nach der Patchcode-GUID, der Produktcode-GUID oder beiden filtern. Hier ein Beispiel:

`dism /image:c:\mountedimages /get-apppatchinfo /patchcode:<{Patchcode-GUID}> /productcode:<{Produktcode-GUID}>`

Neben den Informationen darüber, welche Anwendungspatches angewendet werden können, brauchen Sie meist auch Informationen über die MSI-Anwendungen. Das Argument `/get-apps` listet alle MSI-Anwendungen auf, die im bereitgestellten Abbild installiert sind, sodass Sie damit die GUID jeder Anwendung ermitteln können:

`dism /image:c:\mountedimages /get-apps`

Anschließend können Sie ausführlichere Informationen über installierte Anwendungen abrufen, indem Sie das Argument `/get-appinfo` angeben. Stattdessen können Sie diese Informationen auch filtern, indem Sie die Produktcode-GUID für die Anwendung angeben, an der Sie interessiert sind:

`dism /image:c:\mountedimages /get-appinfo /ProductCode:<{Produktcode-GUID}>`

Wenn Sie keine Produktcode-GUID angeben, liefert `/get-appinfo` detaillierte Informationen über alle installierten MSI-Anwendungen zurück.



Prüfungstipp

Denken Sie daran, dass `/get-apppatches` und `/get-apppatchInfo` nur für installierte Patches (*.msp*-Dateien) gelten, während `/get-apps` und `/get-appinfo` nur Windows Installer-Anwendungen (*.msi*-Dateien) betreffen. Es ist also nicht möglich, mit DISM Informationen über *.exe*- oder *.dll*-Dateien abzurufen. Denken Sie auch daran, dass nur die Windows Installer-Anwendungen, auf die ein Patch angewendet werden kann, angezeigt werden, wenn Sie prüfen, ob ein MSP-Patch angewendet werden kann. Ein und derselbe Patch kann auf viele installierte Anwendungen angewendet werden, und mehrere Patches können auf dieselbe Anwendung angewendet werden.

Hinzufügen von Anwendungen zu einem Abbild

Die DISM-Argumente `/check-apppatch`, `/get-apppatchinfo`, `/get-apppatches`, `/get-appinfo` und `/get-apps` liefern Informationen über Windows Installer-Anwendungen und installierte Patches in einem offline bereitgestellten Abbild. Der nächste Abschnitt beschreibt, wie Sie Paket- (*.cab*) oder eigenständige Windows Update-Installationsdateien (*.msu*) zu einem Abbild hinzufügen und Sicherheitspatches in offline bereitgestellten Abbildern installieren. Sie können auch Windows-Features aktivieren und deaktivieren, aber keine Features oder andere Typen ausführbarer Dateien hinzufügen, zum Beispiel *.exe*-, *.bat*-, *.com*- oder *.vbs*-Dateien. Für DISM gibt es kein Argument namens `/add-apps`.

Wollen Sie eine wichtige Anwendung zu einem Abbild hinzufügen, bevor es verteilt wird, können Sie diese Anwendung auf Ihrem Referenzcomputer installieren, bevor Sie das Abbild aufzeichnen. Müssen Sie dagegen eine Anwendung zu einem bereits vorhandenen Offlineabbild hinzufügen, eignet sich das Tool DISM nicht für diesen Zweck. Verwenden Sie stattdessen den Assistenten zum Hinzufügen von Anwendungen (New Application Wizard) aus MDT 2010; er wird in Lektion 2, »Bereitstellen von Abbildern«, beschrieben.

Sie können mit DISM auch ein Abbild mit einer *Unattend.xml*-Antwortdatei verknüpfen. Eine solche Datei automatisiert die Installation des Abbilds, aber auch Aufgaben, die nach der Installation ausgeführt werden, etwa das Herstellen der Verbindung zu einem Dateiserver, das Installieren von Anwendungen oder das Konfigurieren von Einstellungen. Dieser Ansatz, bei dem Anwendungen und Einstellungen erst nach der Installation angewendet werden, statt sie in das Abbild aufzunehmen, wird als »dünnes Abbild« (thin image) bezeichnet; er wird in Lektion 2 dieses Kapitels beschrieben.

Warten von Betriebssystempaketen

Wenn Sie Systemabbilder entweder für die Verteilung auf mehreren Computern bereithalten oder als Absicherung auf einer startfähigen VHD eines einzelnen Clientcomputers installieren, stellt sich die Frage, wie Sie solche Abbilder auf dem neusten Stand halten, vor allem im Hinblick auf Sicherheitsupdates und -fixes. Andernfalls weist der Computer bekannte Sicherheitslücken auf, sobald er vom neuen Abbild gestartet wird.

Handelt es sich um einen einzelnen Clientcomputer, auf dem Sie, wie in Kapitel 2 beschrieben, ein Systemabbild aufgezeichnet und es auf einer startfähigen VHD installiert haben, stehen mehrere Möglichkeiten zur Auswahl. Der einfachste und oft auch schnellste Weg ist, den Computer von seiner VHD zu starten, sofort Microsoft Update aufzurufen und alle kritischen und empfohlenen Pakete zu installieren. Sie können das von Hand erledigen, aber in einem großen Unternehmen ist es sinnvoller, das Offline Virtual Machine Servicing Tool auf einem Server zu verwenden, auf dem Microsoft System Center Virtual Machine Manager (SCVMM) installiert ist. Der Nachteil dieser Methode besteht darin, dass die Computer online gebracht werden, ohne dass sie die neusten Sicherheitsupdates enthalten. Daher sind sie verwundbar, wenn auch nur für kurze Zeit.

Es ist auch möglich, in regelmäßigen Abständen neue Abbilder Ihres Clientcomputers aufzuzeichnen und das neue Abbild auf der VHD zu installieren. Dabei müssen Sie den Computer unter Windows PE starten, was viel Zeit erfordert, vor allem wenn es regelmäßig geschieht. Diese Methode hat den Vorteil, dass das neue Abbild alle Softwareanwendungen und Benutzerdateien enthält, die zum Computer hinzugefügt worden sind, seit das letzte Abbild aufgezeichnet wurde. Es handelt sich also um eine Art Datensicherung.

Haben Sie ein Abbild für die Verteilung auf sehr viele neue Computer erstellt, können Sie sicherstellen, dass Ihr Referenzcomputer (wie in Kapitel 1 beschrieben) immer auf dem neusten Stand bleibt, und jedes Mal, wenn Sie eine Gruppe Clientcomputer konfigurieren, ein aktuelles Abbild aufzeichnen. Sie können auch MDT 2010 verwenden, um Abbilder zu bearbeiten, wie in Lektion 2 dieses Kapitels beschrieben.

Der oft schnellste und einfachste Weg, Abbilder zu bearbeiten und Pakete zu installieren, besteht allerdings darin, DISM zu verwenden. Mit DISM können Sie auflisten, welche Windows-Pakete in einem bereitgestellten Offlineabbild installiert sind. Sie können Informationen über die installierten Pakete abrufen, Pakete hinzufügen oder entfernen und Windows-Features in einem bereitgestellten Offlineabbild verändern. Dieselben Operationen können Sie mit DISM auch bei einem Onlinebetriebssystem ausführen; allerdings ist es mit Microsoft Update oder WSUS einfacher sicherzustellen, dass beim Onlineabbild alle kritischen und empfohlenen Updates installiert sind.

Schnelltest

- Sie wollen Informationen über zwei Patchdateien namens *Mypatch.msp* und *Otherpatch.msp* aus dem Ordner *C:\Windows\Patches* anzeigen, die in einem Abbild liegen, das unter *D:\Myimages\Mountedimage1* bereitgestellt wurde. Welchen Befehl verwenden Sie?

Antwort zum Schnelltest

- `dism /image:d:\myimages\mountedimagei /check-apppatch /patchlocation:c:\windows\patches\mypatch.msp /patchlocation:c:\windows\patches\otherpatch.msp`

Mithilfe der Paketwartungsbefehle von DISM können Sie in einem offline bereitgestellten Abbild Windows-Pakete installieren, entfernen oder aktualisieren, die als Cabinetdateien (*.cab*) oder eigenständige Windows Update-Installer-Dateien (*.msu*) vorliegen. Microsoft setzt Pakete ein, um Softwareupdates, Service Packs und Language Packs zu verteilen. Pakete können auch Windows-Features (optionale Features für das Kernbetriebssystem) enthalten. Mithilfe der Paketwartungsbefehle können Sie Windows-Features sowohl in einem offline bereitgestellten Abbild als auch in einer laufenden Windows-Installation aktivieren oder deaktivieren.

Sie haben die Möglichkeit, ein Paket in Ihrem Onlineabbild zu identifizieren und es in Ihrem bereitgestellten Offlineabbild zu installieren. Außerdem können Sie ein Feature deaktivieren und wieder aktivieren.

Bei einem Offlineabbild stehen folgende Befehle für die Paketwartung im Betriebssystem zur Verfügung:

```
dism /image:<Pfad_zum_Abbildverzeichnis> [/get-packages | /get-packageinfo |
/add-package | /remove-package ] [/get-features | /get-featureinfo | /enable-feature |
/disable-feature ]
```

Bei einem Onlinebetriebssystem (dem laufenden System) können Sie folgende Befehle für die Paketwartung verwenden:

```
dism /online [/Get-Packages | /Get-PackageInfo | /Add-Package | /Remove-Package]
[/Get-Features | /Get-FeatureInfo | /Enable-Feature | /Disable-Feature]
```

Wollen Sie ein Onlinebetriebssystem mit einem offline bereitgestellten Abbild vergleichen, müssen Sie zuerst alle Pakete und Features auflisten, die in beiden Systemen installiert sind. Dazu verwenden Sie Befehle, die wie im folgenden Beispiel aussehen:

```
dism /online /get-packages > c:\onlinepackages.txt
dism /image:c:\mountedimages /get-packages > c:\offlinepackages.txt
dism /online /get-features > c:\onlinefeatures.txt
dism /image:c:\mountedimages /get-features > c:\offlinefeatures.txt
```

Es empfiehlt sich, die Ausgaben dieser Befehle in Textdateien umzuleiten, um die Listen gut vergleichen zu können. Außerdem sind die Namen einiger Pakete lang und kompliziert, daher ist es nützlich, sie für die Bearbeitung in der Befehlszeile zu kopieren und einzufügen.



Hinweis **Bei Featurenamen wird zwischen Groß- und Kleinschreibung unterschieden**

DISM-Befehle unterscheiden nicht zwischen Groß- und Kleinschreibung, bei den Namen von Features ist diese Unterscheidung aber wichtig.

Nehmen wir an, Sie sollen mehr über die Datei *Package_for_KB970419~31bf3856ad364e35~x86~~6.1.1.0* herausfinden. Dann geben Sie folgenden Befehl ein:

```
dism /online /get-packageinfo /packagename:Package_for_KB970419~31bf3856ad364e35~x86~~
6.1.1.0
```

Die Ausgabe dieses Befehls sehen Sie in Abbildung 3.10.

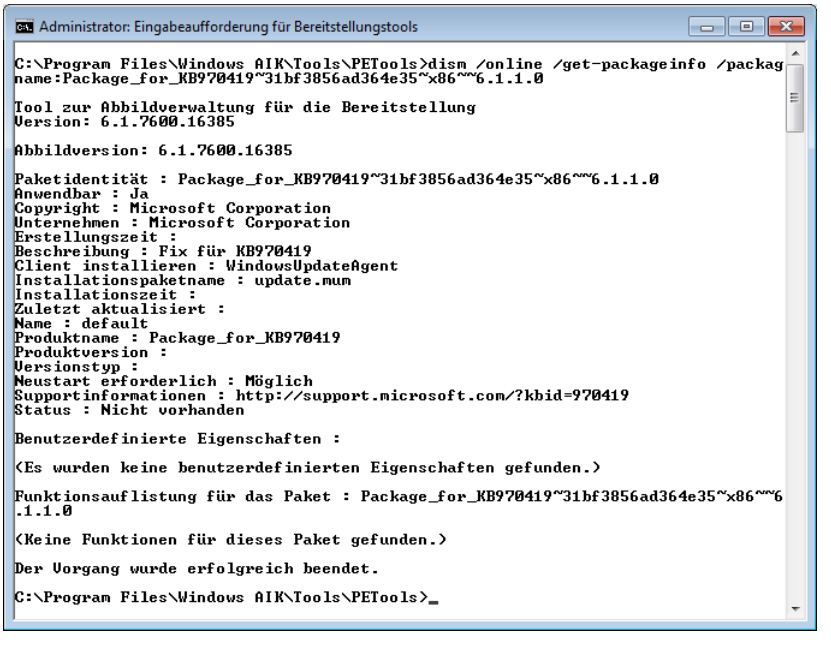


Abbildung 3.10 Informationen über ein Onlinepaket

Es ist nicht möglich, mit dem Argument `/get-packageinfo` Informationen über *.msu*-Dateien zu ermitteln. Sie können es nur für *.cab*-Dateien verwenden.

Nehmen wir an, Sie haben eine Datei namens *Mypackage.cab* heruntergeladen oder erstellt und sie im Ordner *C:\Mypackages* abgelegt. Dieses Paket wollen Sie nun in ein offline bereitgestelltes Abbild einfügen. Dazu verwenden Sie folgenden Befehl:

```
dism /image:c:\mountedimages /add-package /packagepath:c:\mypackages\mypackage.cab
```

DISM prüft bei jedem Paket, ob es angewendet werden kann. Falls es nicht möglich ist, das Paket auf das angegebene Abbild anzuwenden, gibt DISM eine Fehlermeldung zurück. Wollen Sie, dass der Befehl ausgeführt wird, ohne bei jedem Paket zu prüfen, ob es angewendet werden kann, können Sie das Argument `/ignorecheck` anhängen.

Sie können eine *.msu*-Datei nicht entfernen, nachdem sie zu einem Abbild hinzugefügt wurde, aber eine *.cab*-Datei können Sie mit dem Argument `/remove-package` löschen. Mit dem Argument `/get-packages` ermitteln Sie den Paketnamen, wie er im Abbild aufgeführt ist, und im Argument `/packagename` des Befehls geben Sie diesen Namen dann an. Stattdessen können Sie auch das Argument `/packagepath` verwenden und den Pfad zum Quellpaket angeben, das Sie hinzugefügt haben. Ein Beispiel:

```
dism /image:c:\mountedimages /remove-package /packagepath:c:\mypackages\mypackage.cab
```



Prüfungstipp

Wenn Sie ein offline bereitgestelltes Abbild ändern, indem Sie ein Paket hinzufügen oder deinstallieren oder andere Operationen damit ausführen, müssen Sie die Änderungen mithilfe des DISM-Befehls `/commit-wim` im ursprünglichen Quellabbild speichern.

Die DISM-Befehle zum Bearbeiten und Verwalten von Features sind denen für die Arbeit mit Paketen sehr ähnlich. Beispielsweise liefert der folgende Befehl Informationen über das Feature *Chess* in einem laufenden Betriebssystem:

```
dism /online /get-featureinfo /featurename:Chess
```

Mit den Argumenten `/packagename` und `/packagepath` können Sie bei Bedarf nach einem bestimmten Feature in einem Paket suchen. Und mit den Argumenten `/enable-feature` und `/disable-feature` aktivieren oder deaktivieren Sie ein bestimmtes Feature in einem Abbild:

```
dism /image:c:\mountedimages /disable-feature /featurename:Minesweeper
```

Wichtige Faktoren bei der Paketinstallation

Wenn Sie ein Paket in einem Offlineabbild installieren, ändert sich der Paketstatus auf »Installation steht aus«. Das Paket wird installiert, sobald das Abbild gestartet wird und die ausstehenden Onlineaktionen verarbeitet werden. Werden nachfolgende Aktionen angefordert, können sie erst verarbeitet werden, wenn die älteren ausstehenden Onlineaktionen abgeschlossen sind. Wenn sich ein Paket im Status »Installation steht aus« befindet und Sie das Paket bereitstellen, ändert sich sein Status auf »Deinstallation steht aus«, weil das Paket deinstalliert werden muss, bevor es bereitgestellt werden kann.

Manche Pakete benötigen andere Pakete, die vorher installiert werden müssen. Bestehen solche Abhängigkeiten, sollten Sie eine Antwortdatei verwenden, um die erforderlichen Pakete zu installieren. Indem Sie DISM eine Antwortdatei übergeben, können Sie mehrere Pakete in der richtigen Reihenfolge installieren. Microsoft empfiehlt, eine Antwortdatei einzusetzen, um mehrere Pakete zu installieren. Pakete werden in der Reihenfolge installiert, in der sie in der Befehlszeile aufgeführt sind, daher können Sie die Reihenfolge in einer Antwortdatei festlegen.

Wenn Sie mithilfe von DISM alle Featurepakete in einem Windows PE-Abbild auflisten, werden sie immer als ausstehend angezeigt, selbst wenn die Wartungsoperation erfolgreich war. Das ist Absicht, und Sie brauchen keine Maßnahmen zu ergreifen.

Konfigurieren internationaler Einstellungen in einem Abbild

Mit dem Tool DISM können Sie internationale Einstellungen in einem Windows 7-Abbild (oder Windows PE-Abbild) verwalten. Sie können auch vorhandene Einstellungen in einem Offline- oder Onlineabbild abfragen.

Für die Wartung internationaler Einstellungen in einem offline bereitgestellten Abbild stehen folgende Argumente zur Verfügung:

```
dism /image:<Pfad_zum_Offlineabbildverzeichnis> [/get-intl] [/set-uilang |
/et-uilangfallback | /set-syslocale | /Set-UserLocale | /Set-InputLocale |
/Set-AllIntl | /Set-Timezone | /Set-SKUIntlDefaults | /Set-LayeredDriver]
[/Gen-Langini | /Set-SetupUILang | /Distribution]
```

Bei einem laufenden Betriebssystem können Sie den folgenden Befehl verwenden:

```
dism /online /get-intl
```

Dies ist der einzige Befehl für die Wartung internationaler Einstellungen, den Sie bei einem laufenden Betriebssystem ausführen können. Die Ausgabe sehen Sie in Abbildung 3.11.

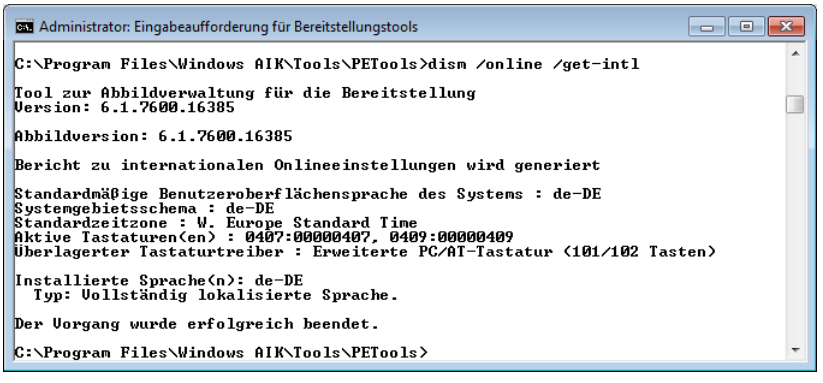

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>dism /online /get-intl
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
Abbildversion: 6.1.7600.16385
Bericht zu internationalen Onlineeinstellungen wird generiert
Standardmäßige Benutzeroberflächensprache des Systems : de-DE
Systemgebietsschema : de-DE
Standardzeitzone : W. Europe Standard Time
Aktive Tastaturen(en) : 0407:00000407, 0409:00000409
Überlagerter Tastaturtreiber : Erweiterte PC/AT-Tastatur (101/102 Tasten)
Installierte Sprache(n): de-DE
Typ: Vollständig lokalisierte Sprache.
Der Vorgang wurde erfolgreich beendet.
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.11 Internationale Einstellungen bei einem Onlinebetriebssystem

Wenn Sie das Argument `/get-intl` bei einem offline bereitgestellten Abbild verwenden und dabei `/distribution` angeben, werden Informationen über internationale Einstellungen und Sprachen in der Bereitstellungsfreigabe angezeigt. Lektion 2 dieses Kapitels beschreibt die Bereitstellungsfreigabe.

Ist die Sprache, die Sie mit `/set-uilang` angeben, nicht im Windows-Abbild installiert, meldet der Befehl einen Fehler. Eine Fallback-Standardsprache wird nur gebraucht, wenn im Argument `/set-uilang` eine teilweise lokalisierte Sprache angegeben ist (beispielsweise Ukrainisch oder Arabisch).

Das Argument `/set-syslocale` legt die Sprache für Nicht-Unicode-Programme (dies ist das sogenannte Systemgebietsschema) und die Schriftartenstellungen fest. Geben Sie den Namen der Sprache und des Gebietsschemas an, die als Standardsprache verwendet werden sollen, zum Beispiel de-DE. Das Argument `/set-userlocale` konfiguriert für einzelne Benutzer Ein-

stellungen, die die Standardsortierreihenfolge und die Standardeinstellungen für die Formatierung von Datum, Uhrzeit, Währung und Zahlen festlegen (zum Beispiel fr-FR).

Schnelltest

- Sie brauchen weitere Informationen über das Paket *Package_for_KB654321~22cf8952ad824e22~x86~~6.1.0.0* in einem WIM-Abbild, das momentan im Ordner *C:\MountedImages* bereitgestellt ist. Welchen Befehl verwenden Sie?

Antwort zum Schnelltest

- `dism /image:c:\mountedimages /get-packageinfo /packagename:Package_for_KB654321~22cf8952ad824e22~x86~~6.1.0.0`

Mit dem Argument `/set-inputlocale` legen Sie das Eingabegebietsschema und das Tastaturlayout fest. Wenn Sie zum Beispiel de-DE als Gebietsschema angeben, wird auch das Standardtastaturlayout für dieses Gebietsschema eingestellt. Wollen Sie im selben Abbild mehrere Tastaturlayouts aktivieren, können Sie die Layouts durch Strichpunkte trennen. Der erste Wert gibt die Standardtastatur an. Wenn Sie beispielsweise deutsche und britische Tastaturen im selben Abbild aktivieren und das deutsche Layout als Standard verwenden wollen, verwenden Sie den folgenden Befehl:

```
dism /image:c:\mountedimages /set-inputlocale:0407:00000407;0410:00010410
```

Abbildung 3.12 zeigt die Ausgabe dieses Befehls.

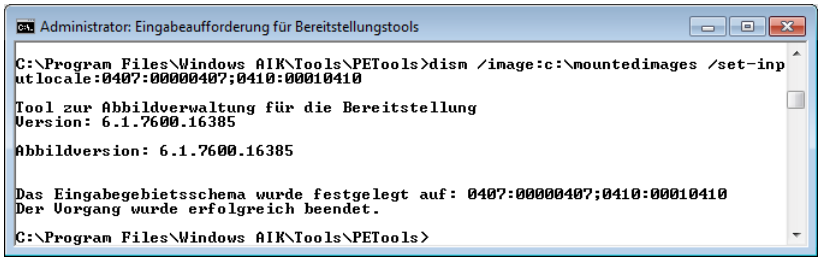


Abbildung 3.12 Festlegen mehrerer Tastaturlayouts

Falls Ihr Abbild einen Tastaturtreiber für japanische oder koreanische Tastaturen braucht, können Sie das Argument `/set-layereddriver` verwenden. In diesem Argument geben Sie einen Wert von 1 bis 6 an, der folgende Bedeutung hat:

1. Erweiterte PC/AT-Tastatur (101/102 Tasten)
2. Koreanische PC/AT-kompatible Tastatur mit 101 Tasten/MS Natural-Tastatur (Typ 1)
3. Koreanische PC/AT-kompatible Tastatur mit 101 Tasten/MS Natural-Tastatur (Typ 2)
4. Koreanische PC/AT-kompatible Tastatur mit 101 Tasten/MS Natural-Tastatur (Typ 3)
5. Koreanische Tastatur (103/106 Tasten)
6. Japanische Tastatur (106/109 Tasten)

Mit dem Argument `/set-allintl` können Sie Benutzeroberflächensprache (User Interface, UI), Systemgebietsschema, Benutzergebietsschema und Eingabegebietsschema auf denselben Wert setzen, zum Beispiel auf de-DE. Wenn Sie `/set-allintl` mit einem der Argumente

kombinieren, die die Sprache oder ein bestimmtes Gebietsschema festlegen, haben die Einzeleinstellungen Vorrang.

Mit dem Argument `/set-skuintldefaults` legen Sie in einem Abbild die System-UI-Standardsprache, die Sprache für Nicht-Unicode-Programme, Standard- und Formatsprache, Eingabegebietsschema, Tastaturlayout und Zeitzonen auf den Windows 7-Standardwert fest, der durch eine Sprachbezeichnung festgelegt wird, beispielsweise de-DE. Beachten Sie, dass `/set-skuintldefaults` nicht den Tastaturtreiber für japanische und koreanische Tastaturen ändert, dafür müssen Sie das Argument `/set-layereddriver` angeben.

Mit dem Argument `/set-timezone` legen Sie die Standardzeitzone fest. Wenn Sie dieses Argument verwenden, prüft DISM, ob die angegebene Zeitzonenbezeichnung für das Abbild gültig ist. Der Name der Zeitzone muss genau mit dem Namen der Zeitzoneneinstellungen im Registrierungsschlüssel *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\TimeZones* übereinstimmen. Wenn Sie eine benutzerdefinierte Zeitzone zu Ihrem Computer hinzufügen, können Sie diese benutzerdefinierte Zeitzonenbezeichnung angeben.



Hinweis Das Befehlszeilentool Tzutil

Auf einem Windows 7-Computer können Sie mit dem Befehlszeilentool Tzutil die Zeitzone des Computers anzeigen. Das Tool Tzutil wird in Windows 7 standardmäßig installiert, es gehört nicht zum Windows AIK.

Verwalten von Windows-Editionen

Windows 7-Editionspakete für jede mögliche Zieledition liegen in einem *Install.wim*-Abbild auf dem Windows 7-Installationsmedium bereit. Dies wird als Editionsfamilienabbild (edition family image) bezeichnet. Weil die Zieleditionen bereitliegen, reicht es aus, ein einziges bereitgestelltes Abbild zu pflegen, um die Updates zu allen Editionen im Abbild hinzuzufügen, in denen sie benötigt werden. Auf diese Weise brauchen Sie weniger Abbilder zu verwalten. Allerdings verlängert sich dadurch die Vorbereitungsdauer oder der Benutzer muss länger waren, bis der Konfigurationsdurchlauf *specialize* abgeschlossen ist.

Mithilfe der Windows-Editionswartungsbefehle können Sie eine Edition von Windows 7 auf eine höhere Edition innerhalb derselben Editionsfamilie aktualisieren. Wenn Sie bei einem Offlineabbild ein Upgrade durchführen, brauchen Sie keinen Product Key. Aktualisieren Sie dagegen ein Onlineabbild auf eine höhere Edition, haben Sie folgende Möglichkeiten, den Product Key hinzuzufügen:

- Geben Sie den Product Key während des OOBE-Durchlaufs (Out-of-Box Experience) ein.
- Verwenden Sie eine Antwortdatei für die unbeaufsichtigte Installation, um den Product Key während des Konfigurationsdurchlaufs *specialize* anzugeben.
- Verwenden Sie DISM mit dem Befehlszeilenargument `/set-productkey`, nachdem Sie die Edition offline konfiguriert haben.

Es stehen folgende Editionswartungsbefehle zur Verfügung, um die Editionen in einem Offlineabbild aufzulisten oder ein Windows-Abbild auf eine höhere Edition zu aktualisieren:

```
dism /image:<Pfad_zum_Abbildverzeichnis> [/get-currentedition | /get-targeteditions |
/set-edition | /set-productkey]
```

Bei einem laufenden Windows 7-Betriebssystem stehen folgende Editionswartungsbefehle zur Verfügung:

```
dism /online [/get-currentedition | /get-targeteditions]
```

Weil dieses Buch sich in erster Linie mit dem Windows 7-Installationsabbild und dem Product Key auf dem gelieferten Installationsmedium beschäftigt, gehen wir hier nicht weiter darauf ein, wie Sie das bereitgestellte Abbild aktualisieren, das Sie generiert, auf einer startfähigen VHD abgelegt und dann im Dateisystem bereitgestellt haben. Wenn Sie die folgenden Befehle mit dem Onlineabbild oder dem installierten Abbild, das Sie in den Übungen weiter unten in dieser Lektion im Dateisystem bereitstellen, ausführen, bearbeiten Sie die Windows 7-Editionen im Online- beziehungsweise bereitgestellten Abbild:

```
dism /online /get-currentedition
dism /image:c:\mountedimages /get-currentedition
```

Es ist auch nicht möglich, Ihre aktuelle Edition auf eine Zieledition zu aktualisieren. Wie in Abbildung 3.13 gezeigt, teilt Ihnen der folgende Befehl das auch mit:

```
dism /online /get-targeteditions
```

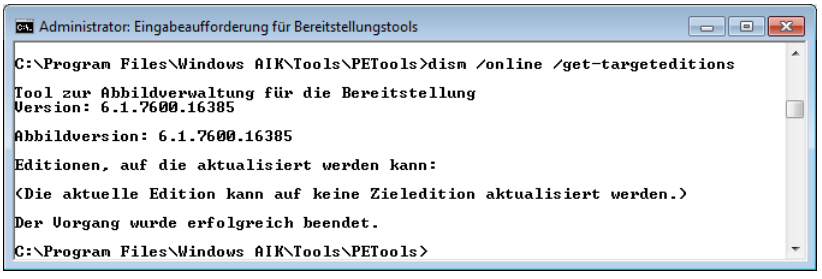


Abbildung 3.13 Es sind keine Zieleditionen verfügbar

Sofern eine Zieledition zur Verfügung steht, können Sie das Argument `/set-edition` ohne `/productkey` angeben, um ein Windows-Offlineabbild auf eine höhere Edition zu aktualisieren. Mit `/get-targeteditions` ermitteln Sie die Editions-ID. Bei einem laufenden Betriebssystem führen Sie ein Upgrade auf eine höhere Edition durch, indem Sie das Argument `/set-edition` zusammen mit `/productkey` angeben, wie im folgenden Befehl:

```
dism /online /set-edition:Ultimate /productkey:12345-67890-12345-67890-12345
```

Warten von Windows PE-Abbildern

Sie können ein Windows PE-Abbild im Dateisystem bereitstellen und dann Pakete, Treiber und Language Packs hinzufügen oder entfernen, genauso wie bei jedem anderen Windows 7-Abbild. DISM stellt auch Argumente bereit, die speziell für ein Windows PE-Abbild gelten. Mithilfe dieser Argumente können Sie die Windows PE-Umgebung vorbereiten, die Profilerstellung aktivieren, Pakete auflisten und das Windows PE-Abbild für die Bereitstellung vorbereiten.

Wenn Sie beispielsweise mit DISM oder ImageX ein Windows PE-Abbild im Ordner *C:\MountedPEImage* bereitgestellt haben, stehen folgende Befehle speziell für Windows PE zur Verfügung:

```
dism /image:c:\mountedpeimage [/get-pesettings | /get-profiling | /get-scratchspace |
/get-targetpath | /set-scratchspace: | /set-targetpath: | /enable-profiling |
/disable-profiling | /apply-profiles:<Pfad_zu_myprofile.txt>]
```



Hinweis DISM-Befehle für Windows PE arbeiten nur mit offline bereitgestellten Abbildern

Sie können mit den Windows PE-Befehlen von DISM keine laufende Onlineversion von Windows PE bearbeiten. Sie müssen ein im Dateisystem bereitgestelltes Windows PE-Abbild verwenden, dessen Pfad Sie mit dem Argument `/image:<Pfad_zum_Abbildverzeichnis>` angeben.

Eine Liste der PE-Einstellungen in einem bereitgestellten Windows PE-Abbild erhalten Sie mit dem folgenden Befehl:

```
dism /image:c:\mountedpeimage /get-pesettings
```

Ob das Windows PE-Profilerstellungstool aktiviert oder deaktiviert ist, verrät der folgende Befehl:

```
dism /image:c:\mountedpeimage /get-profiling
```

Wenn Sie herausfinden wollen, wie viel beschreibbarer Platz auf dem Windows PE-Systemvolume zur Verfügung steht, wenn es im RAM-Disk-Modus gestartet wird (dies ist der sogenannte Entwurfsspeicher auf dem Windows PE-Systemvolume, engl. scratch space), können Sie diesen Befehl ausführen:

```
dism /image:c:\mountedpeimage /get-scratchspace
```

Und der folgende Befehl zeigt an, in welchem Pfad das Stammverzeichnis des Windows PE-Abbilds beim Systemstart liegt (der sogenannte Zielpfad):

```
dism /image:c:\mountedpeimage /get-targetpath
```

Die nächsten Befehle legen die Größe des Entwurfsspeichers und den Zielpfad fest:

```
dism /image:c:\mountedpeimage /set-scratchspace:256
dism /image:c:\mountedpeimage /set-targetpath:D:\WinPEboot
```

Die Größe des Entwurfsspeichers wird in der Einheit MByte angegeben. Gültige Werte sind 32, 64, 128, 256 und 512. Wird das System von Festplatte gestartet, definiert der Zielpfad den Speicherort des Windows PE-Abbilds auf dem Datenträger. Der Pfad muss mindestens 3 Zeichen, aber höchstens 32 Zeichen lang sein. Er muss mit einem Volumebezeichner (*C:*, *D:* und so weiter) beginnen und darf keine Leerzeichen enthalten.

Mithilfe der Dateiprotokollierung (oder Profilerstellung) können Sie in Windows PE 3.0 oder neuer Ihre eigenen Profile generieren. In der Standardeinstellung ist die Profilerstellung deaktiviert. Mit den folgenden Befehlen können Sie die Profilerstellung aktivieren oder wieder deaktivieren:

```
dism /image:c:\mountedpeimage /enable-profiling
dism /image:c:\mountedpeimage /disable-profiling
```

Wenn Sie Profile erstellen, werden sie jeweils in eigenen Ordnern gespeichert und in der Datei *Profile.txt* aufgelistet. Sie können alle Dateien aus einem Windows PE-Abbild löschen, die nicht Teil der benutzerdefinierten Profile sind, und das benutzerdefinierte Profil mit dem Kernprofil vergleichen, um sicherzustellen, dass keine benutzerdefinierten Anwendungs-

dateien und für den Systemstart wichtige Dateien gelöscht werden. Geben Sie dazu einen Befehl ein, der ähnlich wie hier aussieht:

```
dism /image:c:\mountedpeimage /apply-profiles:c:\peprofiles\profile01\profile.txt,
c:\peprofiles\profile02\profile.txt
```

Die Pfade zu einer oder mehreren *Profile.txt*-Dateien werden durch Kommas getrennt als Argumente übergeben.

Schnelltest

1. Sie benötigen eine Liste der Windows PE-Einstellungen in einem Windows PE-Abbild, das im Ordner *C:\Mypeimage* bereitgestellt wurde. Welchen Befehl geben Sie in der erhöhten Eingabeaufforderung für Bereitstellungstools ein?
2. Sie wollen feststellen, wie viel Entwurfsspeicher auf dem Windows PE-Systemvolume in einem Windows PE-Abbild, das im Ordner *C:\Mypeimage* bereitgestellt wurde, zur Verfügung steht, wenn es im RAM-Disk-Modus gestartet wird. Welchen Befehl geben Sie in der erhöhten Eingabeaufforderung für Bereitstellungstools ein?

Antworten zum Schnelltest

1. `dism /image:c:\mypeimage /get-pesettings`
2. `dism /image:c:\mypeimage /get-targetpath`

Befehlszeilenoptionen für unbeaufsichtigte Bearbeitung

Sie können DISM einsetzen, um eine *Unattend.xml*-Antwortdatei auf ein Abbild anzuwenden. Üblicherweise nutzen Sie dieses Feature, wenn Sie mehrere Pakete in einem Abbild installieren wollen. Wie bereits weiter oben in dieser Lektion erwähnt, setzen manche Pakete voraus, dass vorher andere Pakete installiert werden. Microsoft empfiehlt, die richtige Installationsreihenfolge durch Verwendung einer Antwortdatei sicherzustellen. Wenn Sie mithilfe von DISM eine *Unattend.xml*-Antwortdatei auf ein Abbild anwenden, werden die Einstellungen aus der Antwortdatei im Konfigurationsdurchlauf *offlineServicing* (in Kapitel 2 beschrieben) auf das Windows-Abbild angewendet.

Folgende Wartungsbefehle stehen zur Verfügung, um eine *Unattend.xml*-Antwortdatei auf ein bereitgestelltes Windows-Offlineabbild anzuwenden:

```
dism /image:<Pfad_zum_Abbildverzeichnis> /apply-unattend:<Pfad_zu_Unattend.xml>
```

Der folgende Befehl wendet eine *Unattend.xml*-Antwortdatei auf ein laufendes Betriebssystem an:

```
dism /online /apply-unattend:<Pfad_zu_Unattend.xml>
```

Liegt die Datei *Unattend.xml* beispielsweise im Verzeichnis *C:\Windows\Panther*, wenden Sie sie mit dem folgenden Befehl auf ein Offlineabbild an, das in *C:\Mountedimages* bereitgestellt wurde:

```
dism /image:c:\mountedimages /apply-unattend:c:\windows\panther\unattend.xml
```

Abbildung 3.14 zeigt die Ausgabe dieses Befehls. Sie erfahren darin, dass die Antwortdatei angewendet wurde, erhalten aber keine weiteren Informationen.

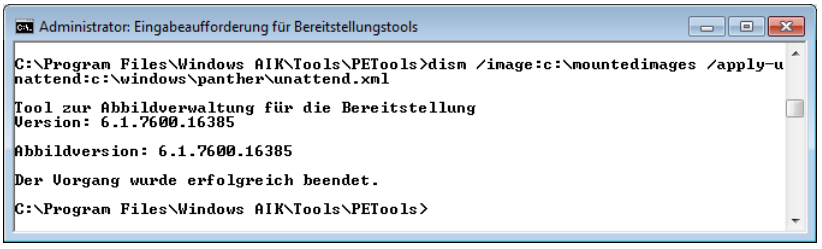


Abbildung 3.14 Anwenden einer Antwortdatei auf ein offline bereitgestelltes Abbild

Verwenden von Antwortdateien für Windows-Abbilder

Die Möglichkeit, eine *Unattend.xml*-Antwortdatei auf ein Abbild anzuwenden, bildet ein leistungsfähiges Werkzeug, um die Abbildbereitstellung zu implementieren und zu konfigurieren. Sie können damit außerdem festlegen, welche Aktionen ausgeführt werden, falls die Bereitstellung fehlschlägt oder erfolgreich abgeschlossen wird.

Wie in Kapitel 2 beschrieben, ist eine Antwortdatei eine XML-Datei (Extensible Markup Language), die Einstellungsdefinitionen und Werte enthält, die während des Windows-Setups benutzt werden. Sie geben die Setupoptionen in einer Antwortdatei an, darunter Angaben zur Partitionierung der Festplatten, den Speicherort des Windows-Abbilds, das installiert werden soll, den verwendeten Product Key und andere benutzerdefinierte Einstellungen für das Windows-Setup. Sie können auch Werte wie die Namen von Benutzerkonten, Anzeigeeinstellungen und Favoriten für den Windows Internet Explorer eintragen. Die Antwortdatei hat gewöhnlich den Namen *Autounattend.xml* und wird mit dem Windows System Image Manager (Windows SIM) erstellt, wie in Kapitel 2 beschrieben. Wollen Sie eine weitere Antwortdatei hinzufügen, um Anwendungen zu installieren oder festzulegen, in welcher Reihenfolge die Pakete installiert werden, verwenden Sie normalerweise den Dateinamen *Unattend.xml*. Wenn Windows SIM eine Windows-Abbilddatei oder Katalogdatei öffnet, werden alle konfigurierbaren Features und Pakete aus diesem Abbild im Fensterabschnitt *Windows-Abbild* angezeigt. Anschließend können Sie die gewünschten Features und Einstellungen zur Antwortdatei hinzufügen.

Schnelltest

- Ihre offline bereitgestellte WIM-Abbilddatei liegt in *C:\Images\Mounted*. Eine Antwortdatei für die unbeaufsichtigte Installation, die Sie mit diesem Abbild verknüpfen wollen, liegt im Dateipfad *C:\Answerfiles\Unattend\Unattend.xml*. Welcher Befehl verknüpft die Antwortdatei mit dem Abbild?

Antwort zum Schnelltest

- `dism /image:c:\images\mounted /apply-unattend:c:\answerfiles\unattend\unattend.xml`

Kapitel 2 hat beschrieben, wie Windows SIM die Eigenschaften und Einstellungen eines ausgewählten Features oder Pakets im Fensterabschnitt *Eigenschaften* anzeigt. Die Featureeinstellungen für jeden Konfigurationsdurchlauf verwalten Sie in diesem Fensterabschnitt. Bei Paketen werden die änderbaren Einstellungen von Windows-Features angezeigt. Einstellungen, die bei einem Feature oder Paket nicht verfügbar sind, werden abgeblendet dargestellt. Veränderte Einstellungen werden durch Fettschrift hervorgehoben. Über die Feature-

einstellungen konfigurieren Sie die Eigenschaften aller Features in einer Windows 7-Installation während des unbeaufsichtigten Setups. Beispielsweise können Sie die Internet Explorer-Featureeinstellung *Home_Page* so konfigurieren, dass beim Start des Browsers eine bestimmte URL geöffnet wird, indem Sie den Standardwert der Einstellung festlegen.

Featureeigenschaften sind nicht konfigurierbare Attribute des Features. Featureeigenschaften werden anders angezeigt, wenn das Feature zur momentan geöffneten Antwortdatei hinzugefügt wird. Feature-IDs identifizieren eindeutig das Feature des Betriebssystems, zu dem die Einstellungen gehören. Die ID enthält Name, Version, Architektur und weitere Angaben zu dem Feature, das im Fensterabschnitt *Windows-Abbild* oder *Antwortdatei* ausgewählt ist. Beispielsweise gibt die ID *Language* den Sprachcode an, und die ID *Name* den Namen des Features oder Pakets. Paketeigenschaften sind nicht konfigurierbare Paketattribute. Zum Beispiel gibt die Paketeigenschaft *Id* die Kennung für das Paket im folgenden Format an: <*Prozessorarchitektur*>_<*Version*>_<*Sprache*>_<*Token des öffentlichen Schlüssels*>_<*Versionsbereich*>.

Paketeinstellungen sind konfigurierbare Attribute eines Pakets, das im Fensterabschnitt *Antwortdatei* aufgeführt ist. Solche Einstellungen können Sie verändern. Beispielsweise definiert die Paketeinstellung *Action*, welche Aktion für das Paket ausgeführt wird. Mögliche Aktionen sind *Install*, *Configure*, *Remove* oder *Stage*.

Einstellungen werden manchmal in Gruppen zusammengefasst, den sogenannten Listenelementen. Ein Listenelement enthält Werte für einen Listenelementtyp und kann mehrere Featureeinstellungen umfassen. Zum Beispiel können Sie mit der Einstellung *FavoritesList* mehrere Favoritenlinks für den Internet Explorer zusammenstellen. Jedes Listenelement muss eine eindeutige Kennung haben, die als Schlüssel (key) des jeweiligen Listenelements bezeichnet wird. Wenn Sie in Windows SIM Listenelemente verwalten, können Sie auf diese Weise ein Listenelement hinzufügen oder entfernen und seine Eigenschaften verändern.

Sie können dieses Konzept ausweiten, um Aufgaben zu automatisieren, die nach der Installation ausgeführt werden. Sie haben die Möglichkeit, eine Antwortdatei nicht nur in Windows SIM, sondern auch in einem Texteditor zu bearbeiten. Wenn Sie beispielsweise daran gewöhnt sind, Batchdateien zu schreiben, mit denen Sie die Anwendungsinstallation automatisieren, können Sie denselben Code in eine Antwortdatei eintragen. Windows SIM erstellt eine binäre Katalogdatei, die alle Einstellungen in einem Windows-Abbild auflistet.

Sie können manuell Code schreiben oder Windows SIM verwenden, um eine Distribution zu erstellen, die Treiber anderer Hersteller, Anwendungen und Microsoft-Pakete wie Sicherheitsbulletins enthält. Um eine Bereitstellungsfreigabe zu erstellen, müssen Sie erst von Hand oder mithilfe von Windows SIM einen Ordner dafür anlegen. Eine *Bereitstellungsfreigabe* (deployment share, auch als distribution share bezeichnet) ist ein freigegebener Windows-Ordner, der folgende Unterordner enthält:

- *OEM Folders*
- *Packages*
- *Out-of-Box Drivers*
- *LangPacks*

Erstellen von Antwortdateien

Microsoft empfiehlt, Windows SIM einzusetzen, um Antwortdateien für die unbeaufsichtigte Installation zu erstellen. Sie können solche Dateien allerdings auch von Hand mit einem Texteditor wie dem Windows-Editor anlegen und bearbeiten. Wenn Sie eine manuell erstellte Antwortdatei verwenden, müssen Sie sie in Windows SIM überprüfen, um sicherzustellen, dass sie funktioniert. Antwortdateien aus Windows XP, Windows Server 2008 oder Windows Vista funktionieren nicht in Windows 7.

Im Allgemeinen ist es am besten, die unterste Ebene eines Features aufzuklappen und nur die Elemente auszuwählen, die Sie konfigurieren wollen. Wollen Sie einen Standardwert übernehmen, brauchen Sie das Element nicht einzutragen, jedenfalls sofern es kein erforderliches Element ist. Wenn Sie Antwortdateien erstellen, müssen Sie wissen, was während der verschiedenen Konfigurationsdurchläufe passiert. Kapitel 2 hat die Konfigurationsdurchläufe beschrieben.



Weitere Informationen Konfigurationsdurchläufe

Weitere Informationen darüber, wie Konfigurationsdurchläufe funktionieren, finden Sie unter *http://technet.microsoft.com/de-de/library/dd744341(WS.10).aspx*.

Wenn Sie Daten hinzufügen, etwa zusätzliche Treiber oder Anwendungen, dürfen Sie auf keinen Fall die Windows-Systemdateien überschreiben. Das könnte das Betriebssystem Ihres Computers beschädigen.



Weitere Informationen Hinzufügen von Anwendungen, Treibern, Paketen, Dateien und Ordnern

Weitere Informationen über das Hinzufügen von Anwendungen, Treibern, Paketen, Dateien und Ordnern finden Sie unter *http://technet.microsoft.com/de-de/library/dd744568(WS.10).aspx*.

Verwenden mehrerer Antwortdateien

Sie können mehrere zusätzliche Antwortdateien (*Unattend.xml*) benutzen, um unterschiedliche benutzerdefinierte Abbilder zu erstellen. Beispielsweise können Sie eine allgemeine Antwortdatei erstellen, die für alle Ihre Systeme eingesetzt wird, und dann während des Überwachungsmodus eine zweite Antwortdatei anwenden, um Datenträgerkonfiguration, Treiber oder Anwendungen zu verändern. Dazu rufen Sie Sysprep (in Kapitel 2 beschrieben) mit dem Argument `/unattend:<Antwortdatei>` auf. Sie können diesen Befehl während des Überwachungsmodus von Hand ausführen oder einen benutzerdefinierten Befehl hinzufügen.



Weitere Informationen Hinzufügen benutzerdefinierter Befehle und Skripts

Weitere Informationen, wie Sie benutzerdefinierte Befehle und Skripts hinzufügen, finden Sie unter *http://technet.microsoft.com/de-de/library/dd744393(WS.10).aspx*.

Übung Bereitstellen eines Offlineabbilds im Dateisystem und Installieren von Language Packs

In dieser Übung setzen Sie sowohl ImageX als auch DISM ein, um ein Abbild im Dateisystem bereitzustellen. Außerdem üben Sie, wie Sie die Bereitstellung eines Abbilds im Dateisystem wieder aufheben. Dann wenden Sie Language Packs auf ein bereitgestelltes Abbild an.

Übung 1 Bereitstellen, Aufheben der Bereitstellung und erneutes Bereitstellen eines Abbilds im Dateisystem

In dieser Übung stellen Sie das Systemabbild *Myimage.wim*, das Sie auf der VHD mit dem Laufwerkbuchstaben *W:* installiert haben, mit dem Tool ImageX im Dateisystem bereit. Sie stellen das Abbild im Ordner *C:\Mountedimages* bereit. Dann heben Sie die Bereitstellung des Ordners im Dateisystem wieder auf. Zuletzt verwenden Sie DISM, um das Abbild im Ordner *D:\Mountedimages* bereitzustellen. Beachten Sie, dass Sie unbedingt einen anderen Ordner verwenden müssen, um das zweite Abbild darin bereitzustellen. Tun Sie das nicht, ist es sinnvoll, den ursprünglichen Ordner zu löschen und neu anzulegen, weil DISM manchmal einen Fehler meldet, obwohl die Bereitstellung des Abbilds im Ordner aufgehoben wurde. Gehen Sie folgendermaßen vor:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Legen Sie einen Ordner namens *C:\MountedImages* an. Sollte dieser Ordner schon vorhanden sein, muss er leer sein.
3. Klicken Sie im Startmenü mit der rechten Maustaste auf *Computer* und wählen Sie den Befehl *Verwalten*. Wählen Sie den Knoten *Datenträgerverwaltung* aus. Falls Datenträger *W:* nicht in der Liste der Volumes aufgeführt wird, müssen Sie mit der rechten Maustaste auf *Datenträgerverwaltung* klicken und den Befehl *Virtuelle Festplatte anfügen* wählen. Wählen Sie die Datei *Myvhd.vhd* aus dem Ordner *C:\VHDs* aus (Abbildung 3.15) und klicken Sie auf *OK*. Nun müsste Laufwerk *W:* aufgelistet werden. Schließen Sie das Dialogfeld *Automatische Wiedergabe*, sofern nötig.

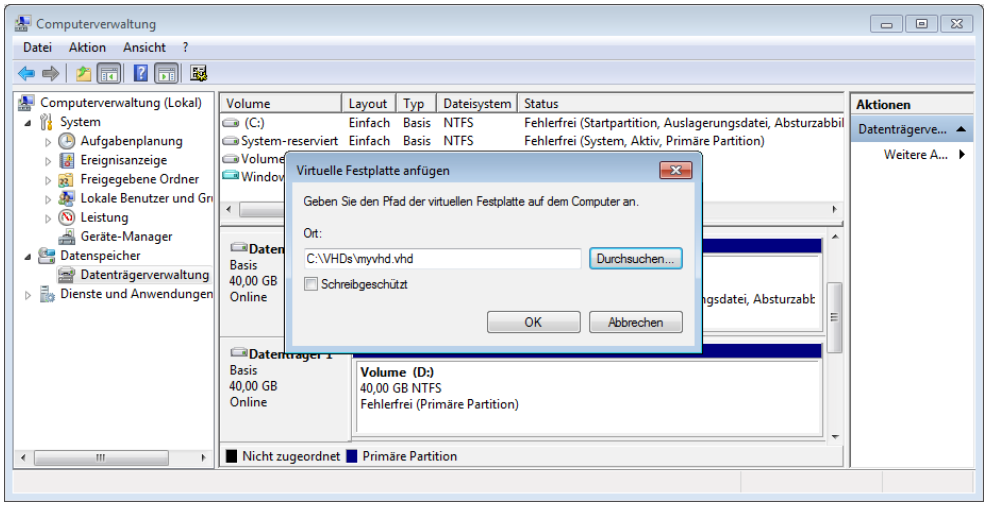


Abbildung 3.15 Anfügen der VHD, wenn sie nicht in der Datenträgerverwaltung aufgeführt wird

4. Klicken Sie im Startmenü auf *Alle Programme*, dann auf *Microsoft Windows AIK*, klicken Sie mit der rechten Maustaste auf *Eingabeaufforderung für Bereitstellungstools* und wählen Sie den Befehl *Als Administrator ausführen*.
5. Geben Sie in der Eingabeaufforderung für Bereitstellungstools den Befehl **imagex /mountrw w:\myimage.wim 1 c:\mountedimages** ein. Abbildung 3.16 zeigt die Ausgabe dieses Befehls.

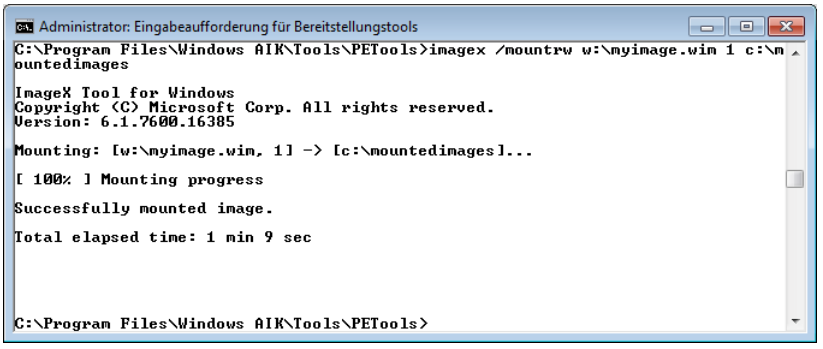

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>imagex /mountrw w:\myimage.wim 1 c:\mountedimages
ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.
Version: 6.1.7600.16385
Mounting: [w:\myimage.wim, 1] -> [c:\mountedimages]...
[100%] Mounting progress
Successfully mounted image.
Total elapsed time: 1 min 9 sec
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.16 Bereitstellen eines WIM-Abbilds im Dateisystem mit ImageX

6. Sie können die Bereitstellung des Abbilds im Dateisystem wieder aufheben und es dann mit dem Tool DISM in einem anderen Ordner bereitstellen. Geben Sie den Befehl **imagex /unmount c:\mountedimages** ein, um die Bereitstellung des Abbilds im Dateisystem aufzuheben. Abbildung 3.17 zeigt die Ausgabe dieses Befehls.

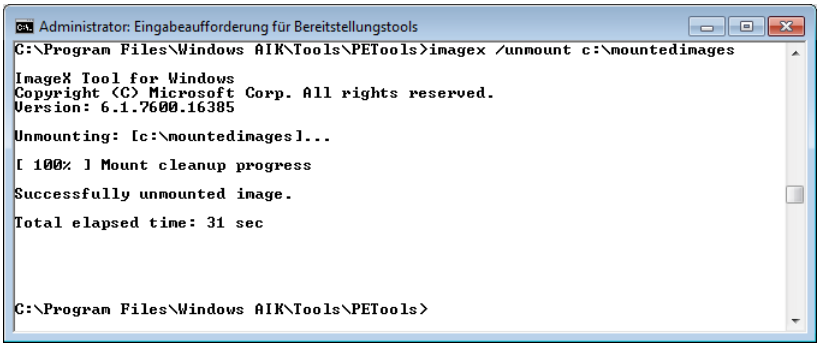

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>imagex /unmount c:\mountedimages
ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.
Version: 6.1.7600.16385
Unmounting: [c:\mountedimages]...
[100%] Mount cleanup progress
Successfully unmounted image.
Total elapsed time: 31 sec
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.17 Aufheben der Bereitstellung eines Abbilds im Dateisystem

7. Legen Sie einen Ordner namens *D:\MountedImages* an. Falls Sie keine zweite Festplatte haben, können Sie auch den Ordner *C:\MountedImages* verwenden; in diesem Fall müssen Sie den Ordner aber löschen und neu anlegen, falls DISM einen Fehler meldet.
8. Stellen Sie das Abbild mit dem Tool DISM im Dateisystem bereit, indem Sie folgenden Befehl eingeben: **dism /mount-wim /wimfile:w:\myimage.wim /index:1 /mountdir:d:\mountedimages.**

9. Testen Sie, ob das Abbild richtig bereitgestellt wurde, indem Sie den Befehl **dism /get-mountedwiminfo** ausführen. Die Ausgabe dieses Befehls sehen Sie in Abbildung 3.18. Beachten Sie, dass der Bereitstellungsordner für das Abbild sich von dem in Abbildung 3.4 weiter oben in dieser Lektion unterscheidet.

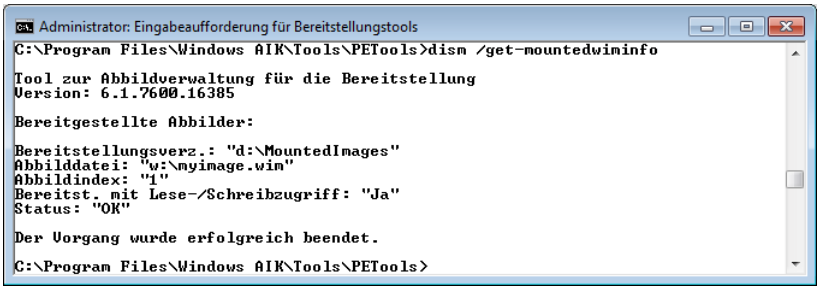


Abbildung 3.18 Ein Abbild wird in *D:\MountedImages* bereitgestellt

Übung 2 Anwenden eines Language Packs auf ein bereitgestelltes Abbild

In dieser Übung wenden Sie das Language Pack de-DE auf Ihr bereitgestelltes Abbild an. Das ist beispielsweise nötig, wenn Sie bereits ein Abbild mit dem Language Pack en-US installiert haben, nun aber in der Lage sein wollen, internationale Einstellungen zu konfigurieren und das Abbild an deutsch- und englischsprachige Benutzer zu verteilen. Beachten Sie, dass Sie nur dann mehrere Language Packs anwenden können, wenn Sie mit Windows 7 Ultimate- oder Enterprise-Abbildern arbeiten. Betrachten Sie diese Übung als allgemeine Anleitung, weil Sie die beschriebenen Schritte für alle Pakete ausführen, die in Form von *.cab*-Dateien verteilt werden. Sie müssen Übung 1 abgeschlossen haben, bevor Sie diese Übung beginnen. Gehen Sie folgendermaßen vor:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Legen Sie einen Ordner namens *C:\Mypackages* an, sofern er noch nicht vorhanden ist.
3. Wechseln Sie in *C:\Program Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\de-de*.
4. Kopieren Sie die Datei *lp_de-de.cab* in den Ordner *C:\Mypackages*.
5. Legen Sie ein Verzeichnis namens *C:\Scratch* an. Dies wird das Entwurfsverzeichnis.
6. Klicken Sie im Startmenü auf *Alle Programme*, dann auf *Microsoft Windows AIK*, klicken Sie mit der rechten Maustaste auf *Eingabeaufforderung für Bereitstellungstools* und wählen Sie den Befehl *Als Administrator ausführen*.
7. Geben Sie den Befehl **dism /image:d:\mountedimages /scratchdir:c:\scratch /add-package /packagepath:c:\mypackages\lp_de-de.cab** ein. Abbildung 3.19 zeigt die Ausgabe dieses Befehls.
8. Übernehmen Sie Ihre Änderungen in das Quellabbild, indem Sie den Befehl **dism /commit-wim /mountdir:d:\mountedimages** ausführen. Sie können nun die Bereitstellung des Abbilds im Dateisystem aufheben, wenn Sie es nicht mehr benötigen.

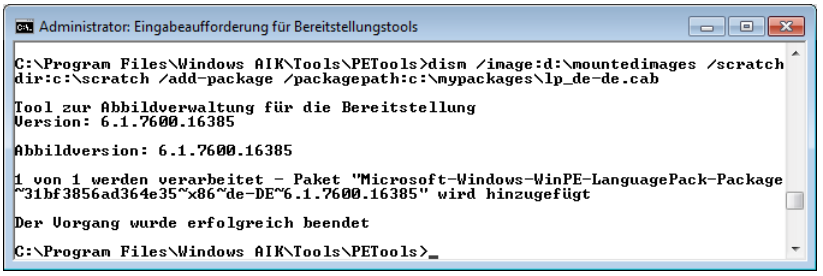

Administrator: Eingabeaufforderung für Bereitstellungstools
C:\Program Files\Windows AIK\Tools\PETools>dism /image:d:\mountedimages /scratch
dir:c:\scratch /add-package /packagepath:c:\mypackages\lp_de-de.cab
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
Abbildversion: 6.1.7600.16385
1 von 1 werden verarbeitet - Paket "Microsoft-Windows-WinPE-LanguagePack-Package
~31bf3856ad364e35~x86~de-DE~6.1.7600.16385" wird hinzugefügt
Der Vorgang wurde erfolgreich beendet
C:\Program Files\Windows AIK\Tools\PETools>

Abbildung 3.19 Hinzufügen eines Language Packs

Zusammenfassung der Lektion

- Sie müssen ein beschreibares Systemabbild (WIM-Datei) in einem Ordner des Dateisystems bereitstellen, um es zu warten. Sie können die Windows AIK-Tools DISM oder ImageX verwenden, um ein Abbild im Dateisystem bereitzustellen.
- Für ein laufendes Onlinebetriebssystem stehen nur sehr wenige Wartungsbefehle zur Verfügung. Sie können immerhin mit dem Tool DISM Informationen über das Onlineabbild ermitteln.
- Mit dem Tool DISM können Sie Pakete, Treiber und Updates zu einem bereitgestellten Abbild hinzufügen. Sie können Informationen über Windows Installer-Anwendungen, Anwendungspakete und Windows-Features abrufen. Sie können Windows-Features deaktivieren oder aktivieren und internationale Einstellungen sowie Windows-Editionen anzeigen und konfigurieren. Sie können Antwortdateien für die unbeaufsichtigte Installation auf ein Abbild anwenden, um die Installation und Aufgaben nach der Installation zu automatisieren. Und schließlich können Sie die Änderungen, die Sie am bereitgestellten Abbild vorgenommen haben, im Quellabbild speichern und die Bereitstellung des Abbilds im Dateisystem wieder aufheben.
- Mit dem Tool DISM können Sie Windows PE-Abbilder im Dateisystem bereitstellen und bearbeiten.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Verwalten eines Systemabbilds vor der Bereitstellung«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie haben die Systemabbilddatei *Install.wim* von Ihrem Windows 7-Installationsmedium in den Ordner *C:\Images* kopiert. Sie haben das Abbild mit dem Index 5 (Windows 7 Ultimate) im Ordner *D:\Mount* bereitgestellt. Sie wollen nun Treiber anderer Hersteller, die Sie in *C:\Drivers\Printer* und *C:\Drivers\Scanner* gespeichert haben, zum bereitgestellten Abbild hinzufügen. Welche der folgenden DISM-Befehle verwenden Sie? (Wählen Sie alle zutreffenden Antworten aus.)

A. `dism /image:c:\images /add-driver /driver:c:\drivers /recurse`

B. `dism /image:d:\mount /add-driver /driver:c:\drivers /recurse`

C. `dism /image:c:\images /add-driver /driver:c:\drivers\printer /driver: c:\drivers\scanner`

D. `dism /image:d:\mount /add-driver /driver:c:\drivers\printer /driver: c:\drivers\scanner`

2. Sie wollen feststellen, wie viel beschreibbarer Speicher auf einem Windows PE-Systemvolume zur Verfügung steht, wenn es im RAM-Disk-Modus gestartet wird. Das Windows PE-Abbild wurde im Ordner *D:\PEMount* bereitgestellt. Welchen Befehl verwenden Sie?

   A. `dism /image:d:\pemount /get-scratchspace`

   B. `dism /image:d:\pemount /get-targetpath`

   C. `dism /image:d:\pemount /get-profiling`

   D. `dism /image:d:\pemount /enable-profiling`

3. Welches der folgenden DISM-Argumente können Sie für ein laufendes Onlinebetriebssystem verwenden?

   A. `/set-syslocale`

   B. `/set-userlocale`

   C. `/set-inputlocale`

   D. `/get-intl`

4. Sie haben eine Antwortdatei namens *Unattend.xml* im Ordner *C:\Textfiles\Answer* erstellt. Sie wollen sie nun auf ein Abbild anwenden, das im Ordner *C:\Mount* bereitgestellt wurde. Welchen Befehl verwenden Sie?

   A. `dism /image:c:\textfiles\answer /apply-unattend:c:\mount\unattend.xml`

   B. `dism /image:c:\mount /apply-unattend:c:\textfiles\answer\unattend.xml`

   C. `dism /image:c:\mount /apply:c:\textfiles\answer\unattend.xml`

   D. `dism /image:c:\mount /apply-answer:c:\textfiles\answer\unattend.xml`

5. Sie brauchen ausführliche Informationen über alle Windows Installer-Anwendungen (*.msi*), die im WIM-Abbild installiert sind, das im Ordner *C:\Mount* bereitgestellt wurde. Welchen Befehl verwenden Sie?

   A. `dism /online /get-packageinfo`

   B. `dism /image:c:\mount /get-featureinfo`

   C. `dism /image:c:\mount /get-appinfo`

   D. `dism /image:c:\mount /get-apppatchinfo`

Lektion 2: Bereitstellen von Abbildern

Abbilder auf sehr vielen Computern bereitzustellen, ist eine wichtige Aufgabe in der Unternehmensumgebung. Werden 100 neue Clientcomputer angeschafft, sollen Sie das aktuelle Betriebssystem, Treiber, Language Packs und so weiter fehlerfrei und mit wenig oder sogar ganz ohne Benutzereingaben bereitstellen. Kommt ein neuer Benutzer hinzu, für den eine einzelne Arbeitsstation angeschafft wird, sollen Sie diesen Computer effizient ans Netzwerk anschließen und das passende Abbild darauf bereitstellen.

Leider bleibt nichts unverändert, und wenige Dinge veralten so schnell wie Systemabbilder. Ein neuer Treiber wird veröffentlicht oder es kommt eine neue Version von Software, die in Ihrer Organisation täglich benutzt wird. Oder das Unternehmen führt weitere Hardware ein, die nicht Plug & Play-fähig ist. Neue Updates scheinen täglich einzutreffen (auch wenn sie meist am Dienstag veröffentlicht werden). Einige davon sind wichtige Sicherheitsupdates; wenn Sie Ihr Abbild ohne diese Updates bereitstellen, sind Ihre Clients gefährdet.

Diese Lektion beschreibt, wie Sie Abbilder über ein Netzwerk bereitstellen, Updates in Abbilder einspielen und Abbilder auf Clients bereitstellen, von denen einige automatisch über das Netzwerk starten können, andere aber nicht. Es stellt die Tools vor, die Ihnen zur Verfügung stehen, um diese wichtige administrative Aufgabe effizient zu erledigen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Hinzufügen von Updates, Anwendungen und Language Packs zu einem Online- oder Offlinedatenträgerabbild mit MDT und Aktualisieren der WIM-Abbilddateien, damit sie auf dem neusten Stand bleiben
- Anlegen einer Bereitstellungsfreigabe für Bereitstellungsabbilder; Konfigurieren der Bereitstellungsfreigabe und Hinzufügen von Tasksequenzen
- Beschreiben der Servertools wie WDS und SCCM 2007, die mit MDT 2010 zusammenarbeiten oder unabhängig Systemabbilder bereitstellen
- Beschreiben der Anforderungen für Lite Touch Installation (LTI) und Zero Touch Installation (ZTI)

Veranschlagte Zeit für diese Lektion: 50 Minuten

Arbeiten mit dem Microsoft Deployment Toolkit

Kapitel 2 hat das Microsoft Windows Deployment Toolkit (MDT) 2010 kurz vorgestellt. Dieses Toolkit ist der Microsoft Solution Accelerator für die Bereitstellung von Betriebssystemen und Anwendungen. Es bietet eine Reihe neuer Features, darunter flexible Treiberverwaltung, optimierte Transaktionsverarbeitung und Zugriff auf Bereitstellungsfreigaben von beliebigen Standorten aus. In einer Unternehmensumgebung setzen Sie das MDT auf Abbild- und Bereitstellungsservern ein, um die automatische Bereitstellung von Windows 7 (oder anderen Versionen) auf Clientcomputern zu implementieren.

MDT 2010 fasst die Tools und Prozesse, die Sie für die Desktop- und Serverbereitstellung brauchen, in einer Bereitstellungskonsole zusammen. Es umfasst einen Bereitstellungs-Accelerator der vierten Generation, der sich in die Microsoft-Bereitstellungstechnologien integriert, sodass ein konsolidierter Ablauf für die Abbilderstellung und die automatische Installation entsteht. Anders ausgedrückt: Es macht die Erstellung und Bereitstellung eines

Systemabbilds viel einfacher. Microsoft weist darauf hin, dass MDT detaillierte Leitfäden und Hilfsmaterial für alle Organisationsrollen enthält, die an umfangreichen Bereitstellungsprojekten beteiligt sind. Es stellt in einer gemeinsamen Bereitstellungskonsole einheitliche Tools und Prozesse bereit, die Sie für Desktop- und Serverbereitstellungen nutzen, wodurch sich der Zeitaufwand für die Bereitstellung verringert. Das Toolkit stellt standardisierte Desktop- und Serverabbilder sowie verbesserte Sicherheit und Möglichkeiten zur kontinuierlichen Konfigurationsverwaltung bereit.

Sie können MDT 2010 mit der LTI-Methode nutzen oder die Installation mithilfe von ZTI vollständig automatisieren. ZTI greift auf Microsoft System Center Configuration Manager (SCCM) 2007 mit dem Operating System Deployment Feature Pack zurück, außerdem muss dafür ein Server mit Microsoft SQL Server 2005 oder SQL Server 2008 im Netzwerk verfügbar sein. LTI können Sie auch benutzen, wenn keine Softwareverteilungstools vorhanden sind, um nicht-PXE-fähige (Pre-Execution Environment) Clients bereitzustellen. Allerdings müssen Sie es mit WDS kombinieren, wenn Sie die Bereitstellung auf PXE-kompatiblen Clients durchführen wollen. In den Übungen am Ende dieser Lektion installieren Sie MDT 2010 auf dem Computer *Canberra*, um sich mit den Features dieses Toolkits vertraut zu machen. Im tatsächlichen Einsatz verwenden Sie dafür normalerweise aber einen Bereitstellungsserver, auf dem die WDS-Serverrolle installiert ist. Unabhängig davon, welche Bereitstellungsmethode Sie einsetzen, setzt MDT 2010 voraus, dass das Windows AIK installiert ist.



Hinweis Systems Management Server

Im Unterschied zur vorherigen MDT-Version (MDT 2008 Update 1) kann MDT 2010 nicht Microsoft Systems Management Server (SMS) 2003 nutzen, um ZTI zu implementieren.

Microsoft bietet MDT 2010 in zwei Versionen an, um die Installation des Solution Accelerators auf x64- und x86-Hosts zu ermöglichen. Die Dokumentation zu MDT 2010 steht auch als separater Download zur Verfügung; die Einführung enthält unter anderem Schritt-für-Schritt-Anleitungen, wie Sie Windows 7 installieren, sodass Sie sich schnell in MDT 2010 einarbeiten können.

Neue Features in MDT 2010

MDT 2010 stellt eine Reihe neuer Features für LTI-basierte Bereitstellungen zur Verfügung. Die ZTI-basierte Bereitstellung, bei der SCCM 2007 benutzt wird, wurde erst vor Kurzem (in MDT 2008 Update 1) eingeführt. Sie hat sich kaum verändert, allerdings kann ZTI nicht mehr mithilfe von SMS 2003 implementiert werden.

Das MDT 2010 umfasst folgende neue Features:

- Unterstützung für Windows 7
- Unterstützung für Windows Server 2008 R2
- Unterstützung für Windows AIK Version 2.0
- Unterstützung für Windows User State Migration Toolkit (USMT) Version 4.0. Besonders werden folgende neue Features von USMT 4.0 in LTI-basierten Bereitstellungen unterstützt:
  - USMT 4.0-Hardlinkmigration
  - USMT 4.0-Schattenkopien

- Unterstützung für das Tool DISM
- Unterstützung für Windows PE Version 3.0
- Unterstützung für das Tool zum Verwalten von Startkonfigurationsdaten (Boot Configuration Data, BCD) und das Befehlszeilenprogramm BCDEdit
- Unterstützung für die standardmäßige Festplattenpartitionskonfiguration in Windows 7. In MDT 2010 legt die Festplattenpartitionskonfiguration für Windows 7 das Betriebssystem auf Festplatte 0, Partition 2 und die Systempartition auf Festplatte 0, Partition 1.



Weitere Informationen Neue Features in MDT 2010

Weitere Informationen über die neuen Features von MDT 2010 beschreibt die Datei *What's New in MDT 2010 Guide.docx*. In den Übungen weiter unten in dieser Lektion ist beschrieben, wie Sie diese Datei herunterladen. Stattdessen können Sie ihren Inhalt auch im Information Center lesen, das Sie über die Deployment Workbench aufrufen.

Programmordner von MDT

Wenn Sie MDT 2010 installieren, werden mehrere Unterordner im MDT 2010-Programmordner *%SysVol%\Program Files\Microsoft Deployment Toolkit* (meist *C:\Program Files\Microsoft Deployment Toolkit*) angelegt. Tabelle 3.3 beschreibt diese Unterordner.

Tabelle 3.3 MDT 2010-Programmordner

Unterordner	Beschreibung
Bin	Enthält das MMC-Snap-In *Deployment Workbench* und Unterstützungsdateien.
Control	Enthält Konfigurationsdaten für die Deployment Workbench. Direkt nach der Installation ist dieser Ordner gewöhnlich leer.
Documentation	Enthält Dokumentation und Hilfsmaterial wie einen Startbildschirm für MDT 2010.
Downloads	Enthält eine Liste der Features, die von der Deployment Workbench heruntergeladen wurden.
Management Pack	Enthält Management Pack-Dateien, zum Beispiel *Microsoft.Deployment.Management.Pack.xml*.
Samples	Enthält Beispielskripts für Tasksequenzen (beispielsweise *ZTICache.vbs*) und Hintergrundbilder für den Windows PE-Desktop.
SCCM	Enthält Vorlagen für Tasksequenzen und Automatisierungsobjekte, die bei der SCCM-Integration benutzt werden, zum Beispiel *Deploy_SCCM_Scripts.vbs*.
Scripts	Enthält Skripts, die von der Deployment Workbench benutzt werden, beispielsweise *ComponentCheck_scripts.vbs*.
Templates	Enthält Vorlagendateien, die von der Deployment Workbench benutzt werden.

Arbeiten mit der Deployment Workbench

Sobald Sie MDT 2010 installiert haben, können Sie die Deployment Workbench aus dem Microsoft Deployment Toolkit starten. Dieses Tool verwenden Sie in den Übungen dieser Lektion, um ein Windows 7-Systemabbild bereitzustellen. Der Rest dieses Abschnitts gibt einen Überblick über die Features, die das Tool zur Verfügung stellt. In der Deployment Workbench haben Sie unter anderem Zugriff auf folgende Elemente:

- **Information Center** Hier können Sie die MDT 2010-Dokumentation lesen, darunter Informationen über die Neuerungen in MDT 2010 und die Features, die vorausgesetzt werden.
- **Bereitstellungsfreigabe (Deployment Shares)** Hier führen Sie alle Aufgaben aus, die nötig sind, um ein Betriebssystemabbild bereitzustellen (Abbildung 3.20). Dabei erstellen Sie beispielsweise ein Bereitstellungsverzeichnis und kopieren die benötigten Abbilddateien hinein.

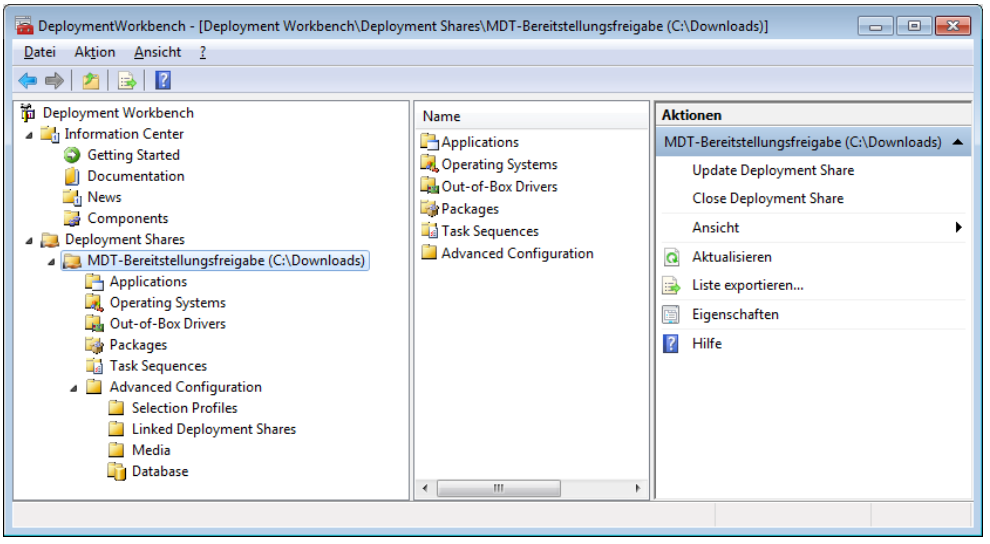


Abbildung 3.20 Aufbau einer Bereitstellungsfreigabe

- **Tasksequenzen (Task Sequences)** In der Detailansicht des Knotens *Task Sequences* werden die Tasksequenzen aufgelistet. Sie erstellen eine Tasksequenz, indem Sie mit der rechten Maustaste auf *Task Sequences* klicken und den Befehl *New Task Sequence* wählen. Eine vorhandene Tasksequenz konfigurieren Sie, indem Sie in der Detailansicht den entsprechenden Eintrag mit der rechten Maustaste anklicken und den Befehl *Eigenschaften* wählen.
- **Erweiterte Konfiguration (Advanced Configuration)** Wenn Sie diesen Zweig aufklappen, sehen Sie unter anderem Auswahlprofile, Bereitstellungsfreigaben und Datenbankelemente. In der Detailansicht können Sie die Eigenschaften der jeweils ausgewählten Elemente ansehen und bearbeiten.



Vorsicht Öffnen Sie nur eine Instanz der Deployment Workbench

Microsoft empfiehlt, nur eine einzige Instanz der Deployment Workbench zu öffnen. Wenn Sie mehrere Instanzen gleichzeitig benutzen, kann unerwartetes Verhalten die Folge sein.

Auswählen einer Abbildstrategie

Wenn Sie ein Abbild in einer Unternehmensumgebung verteilen, sollten Sie nach Möglichkeit versuchen, eine Standardkonfiguration zu entwickeln, die auf einem gemeinsamen Abbild für jede Version eines Betriebssystems aufbaut. In großen Organisationen ist es sinnvoll, ein gemeinsames Abbild auf alle Computer anzuwenden, unabhängig davon, wo und wann das geschieht. Anschließend kann das Abbild schnell angepasst werden, um den Benutzern die benötigten Dienste zur Verfügung zu stellen.

Die meisten Organisationen erstellen und pflegen viele Abbilder. Sie können die Zahl unterschiedlicher Abbilder aber dadurch verringern, indem Sie Disziplin beim Hardwarekauf verlangen und leistungsfähige Skripttechniken nutzen. Sie können die benötigte Infrastruktur für die Softwareverteilung nutzen, um Anwendungen bereitzustellen und Ihre Abbilder aktualisiert zu halten.

Sie können einen der folgenden Abbildtypen verwenden, je nachdem, ob Sie nur Betriebssysteme auf sehr vielen Computern installieren, ob Sie gleichzeitig mit dem Betriebssystem Anwendungen, Language Packs und andere Dateien bereitstellen oder ob Sie für Datensicherungs- und Failoverzwecke ein Abbild auf der VHD eines einzelnen Computers bereitstellen:

- Thick-Abbild
- Thin-Abbild
- Hybridabbild

Thick-Abbilder enthalten neben dem Betriebssystem auch noch Kernanwendungen, Language Packs und andere Dateien. Wenn Sie ein Datenträgerabbild erstellen, das Kernanwendungen und Language Packs enthält, können Sie in einem einzigen Schritt das Datenträgerabbild und die Kernanwendungen auf dem Zielcomputer bereitstellen, inklusive Sprachunterstützung für alle gewünschten Gebietsschemas. Außerdem sind Thick-Abbilder oft billiger zu entwickeln, weil sie in vielen Fällen keine außergewöhnlichen Skripttechniken benötigen. Sie können mit MDT 2010 Thick-Abbilder erstellen, die mit wenig oder sogar ganz ohne Skripts auskommen. Wenn Sie Thick-Abbilder verwenden, stehen Kernanwendungen und Language Packs sofort nach dem ersten Start zur Verfügung.

Thick-Abbilder haben den Nachteil, dass sie neu gebaut, getestet und verteilt werden müssen, wenn sie mit einer neuen Version einer Anwendung oder einem Language Pack aktualisiert werden. Erstellen Sie Thick-Abbilder, die Kernanwendungen und Language Packs umfassen, müssen Sie diese Komponenten während der Abbilderstellung installieren. Thick-Abbilder sollten Sie einsetzen, wenn Sie WIM-Dateien für Datensicherung und Failover auf startfähigen VHDs von einzelnen Computern mit Windows 7 Enterprise oder Ultimate verwenden.

Ein Thin-Abbild ist viel einfacher zu pflegen und zu speichern. Es enthält nur wenige Kernanwendungen oder Language Packs (wenn überhaupt). Anwendungen und Language Packs werden getrennt vom Datenträgerabbild installiert. Wenn Sie das Netzwerk nicht zu sehr beanspruchen dürfen, können Sie beispielsweise den intelligenten Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS) verwenden. Viele Infrastrukturen für Softwareverteilung nutzen diese Technik.

Der größte Nachteil von Thin-Abbildern ist, dass ihre Entwicklung schwieriger ist. Wenn Sie Anwendungen und Language Packs außerhalb des Datenträgerabbilds bereitstellen, brauchen Sie Skripting und eine Infrastruktur für die Softwareverteilung. Und wenn Sie Thin-Abbilder einsetzen, stehen Kernanwendungen und Language Packs nicht sofort beim ersten Start zur Verfügung. In manchen Szenarien wird das als Sicherheitsrisiko eingestuft.

Sofern Sie Thin-Abbilder erstellen, die keine Anwendungen oder Language Packs enthalten, sollte Ihre Organisation über eine Verwaltungsinfrastruktur wie SCCM 2007 verfügen, um Anwendungen und Language Packs bereitzustellen. Sie sollten diese Infrastruktur nutzen, um die Anwendungen und Language Packs bereitzustellen, sobald das Thin-Abbild installiert ist.

Hybridabbilder sind eine Mischung aus Thin- und Thick-Abbildern. Bei einem Hybridabbild wird das Datenträgerabbild so konfiguriert, dass Anwendungen und Language Packs bei der ersten Ausführung installiert werden, diese Komponenten aber automatisch aus einer Netzwerkquelle bezogen werden. Hybridabbilder bieten die meisten Vorteile der Thin-Abbilder, ihre Entwicklung ist aber nicht so aufwendig und sie setzen keine Infrastruktur für die Softwareverteilung voraus. Allerdings dauert die Installation damit länger.

Sie können aus einem Thin-Abbild ein Thick-Abbild für einen einmaligen Einsatz erstellen, indem Sie ein entsprechendes Referenzabbild zusammenstellen. Anschließend fügen Sie Kernanwendungen und Language Packs hinzu, zeichnen sie auf, testen sie und verteilen ein Thick-Abbild, das auf dem Thin-Abbild basiert. Achten Sie aber auf Anwendungen, die sich nicht im Rahmen der Abbilderstellung eines Datenträgers installieren lassen.

Hybridabbilder speichern Anwendungen und Language Packs im Netzwerk, enthalten aber Befehle, um sie zu installieren, sobald das Datenträgerabbild bereitgestellt wird. Dieser Vorgang unterscheidet sich von der Installation der Anwendungen und Language Packs im Datenträgerabbild, weil die Installationsprozesse, die während der Abbilderstellung normalerweise ausgeführt werden, auf einen späteren Zeitpunkt verschoben werden.

Verwalten und Verteilen von Abbildern mit MDT 2010

Wenn Sie mit dem Programm MDT 2010 ein Abbild in einer Bereitstellungsfreigabe erstellen, ist es oft notwendig, Updates, Language Packs und Anwendungen hinzuzufügen. Mit dem Tool MDT 2010 können Sie das sowohl offline als auch online erledigen.

In einer Unternehmensumgebung werden Sie wohl kaum einen Computer, der unter dem Clientbetriebssystem Windows 7 läuft, als Distributionsserver einsetzen, aber es ist möglich, MDT 2010 darauf zu installieren und damit Bereitstellungsfreigaben und Tasksequenzen zu erstellen. Sie können MDT 2010 beispielsweise auf einem Windows 7-Computer betreiben, um in einem kleinen Testnetzwerk Clientbetriebssysteme zu installieren. Das ist sogar in einer kleinen Arbeitsgruppenumgebung möglich, allerdings empfiehlt Microsoft, für diesen Zweck einen Server zu verwenden, der unter Windows Server 2008 läuft.

MDT 2010 bietet die Möglichkeit, WIM-Abbilder zu verwalten und zu verteilen. Wenn Sie ein Windows 7-Betriebssystem auf sehr vielen Clientcomputern konfigurieren wollen, können Sie ein WIM-Abbild (*Install.wim*) vom Installationsmedium kopieren. Je nachdem, welche Computertypen in Ihrer Umgebung im Einsatz sind und welche Hardware sie ver-

wenden, ist es unter Umständen nötig, Gerätetreiber von Hardwareanbietern hinzuzufügen, damit das System seinen vollen Funktionsumfang bietet. Außerdem müssen Sie oft Updates zum Abbild hinzufügen.

Sie können das Betriebssystemabbild entweder über die LTI- oder die ZTI-Methode an die Clientcomputer verteilen. Bei ZTI müssen Sie SCCM 2007 sowie SQL Server 2005 oder SQL Server 2008 in Ihrem Netzwerk zur Verfügung haben.

Wie in Kapitel 2 beschrieben, können Sie Windows 7 auf einem Referenzcomputer installieren, zusammen mit der Software, die Sie in das Abbild aufnehmen wollen. Dann bereiten Sie den Computer mit dem Tool Sysprep für die Abbilderstellung vor. Anschließend starten Sie unter Windows PE und generieren mit dem Windows AIK-Tool ImageX eine WIM-Abbilddatei, die Sie schließlich in die MDT-Bereitstellungsfreigabe legen.



Hinweis Zwei Arten von Referenzcomputern

Wenn Sie den Ansatz eines Thin-Abbilds wählen und mit der Deployment Workbench Updates, Treiber, Pakete, Language Packs und Anwendungen zu einem Betriebssystemabbild hinzufügen, das Sie vom Installationsmedium kopiert haben, sollten Sie das fertige Abbild immer auf einem einzelnen Clientcomputer bereitstellen und es gründlich testen, bevor Sie es auf mehreren Clients bereitstellen. Der einzelne Clientcomputer, den Sie für die Tests benutzen, wird ebenfalls oft als *Referenzcomputer* (reference computer) bezeichnet. Verwechseln Sie einen Referenzcomputer, den Sie von Hand installieren, konfigurieren und testen, bevor Sie sein Abbild aufzeichnen (beschrieben in Kapitel 2), nicht mit dem Referenzcomputer, den Sie für Testzwecke mithilfe des Abbilds installieren, das Sie in MDT 2010 konfiguriert haben.

Schnelltest

- Sie haben Windows AIK und MDT 2010 installiert. Welche zusätzlichen Softwaretools brauchen Sie, um ZTI zu implementieren?

Antwort zum Schnelltest

- SCCM 2007 und SQL Server

Anlegen einer Bereitstellungsfreigabe

Wenn Sie mit MDT 2010 ein Systemabbild bereitstellen, besteht Ihr erster Schritt darin, eine Bereitstellungsfreigabe anzulegen, in der dieses Abbild bereitliegt. Das erledigen Sie in den Übungen weiter unten in dieser Lektion. Dieser Abschnitt beschreibt, wie der Vorgang im Prinzip abläuft. Die Bereitstellungsfreigabe enthält alle Daten und Einstellungen, die MDT 2010 benutzt. Gehen Sie folgendermaßen vor, um eine neue Bereitstellungsfreigabe zu erstellen:

1. Öffnen Sie die Deployment Workbench, klicken Sie mit der rechten Maustaste auf *Deployment Shares* und wählen Sie den Befehl *New Deployment Share*.
2. Geben Sie auf der Seite *Path* des Assistenten den Pfad der neuen Bereitstellungsfreigabe im lokalen Dateisystem ein.
3. Geben Sie auf der Seite *Share* den Freigabenamen und auf der Seite *Descriptive Name* den Anzeigenamen für die Bereitstellungsfreigabe ein. Auf den weiteren Assistenten-

seiten können Sie zusätzliche Standardeinstellungen für die Bereitstellungsfreigabe vornehmen, bevor Sie sie mit einem Klick auf *Finish* erstellen lassen.

Ihre neue Bereitstellungsfreigabe können Sie nun in der Deployment Workbench konfigurieren, um folgende Aufgaben auszuführen:

- Hinzufügen, Entfernen und Konfigurieren von Betriebssystemen
- Hinzufügen, Entfernen und Konfigurieren von Anwendungen
- Hinzufügen, Entfernen und Konfigurieren von Betriebssystempaketen, darunter Updates und Language Packs
- Hinzufügen, Entfernen und Konfigurieren von Out-of-Box-Gerätetreibern

Die Quelldateien für diese Tasks sind im Ordner der Bereitstellungsfreigabe gespeichert. Sie werden während des Konfigurationsprozesses mit Tasksequenzen verknüpft. Die Deployment Workbench speichert Metadaten über Betriebssysteme, Anwendungen, Betriebssystempakete und Out-of-Box-Gerätetreiber im Unterordner *Control*.

Hinzufügen eines Betriebssystemabbilds

Wenn Sie ein benutzerdefiniertes Abbild erstellt haben, entweder durch Abbilderstellung eines Referenzcomputers (wie in Kapitel 2 beschrieben) oder durch Abbilderstellung einer Clientarbeitsstation, die unter Windows 7 Enterprise oder Ultimate läuft, um dieses Abbild zu Failoverzwecken auf einer startfähigen VHD zu speichern, können Sie dieses Betriebssystemabbild zur Bereitstellungsfreigabe auf einem Computer hinzufügen, auf dem MDT 2010 läuft. Dies ist normalerweise ein Thick-Abbild, weil Ihr Referenzabbild Updates, Anwendungen, Treiber und Pakete (darunter Language Packs) enthält. Sie können auch WDS-Abbilder von WDS-Servern zur Bereitstellungsfreigabe hinzufügen.

Am häufigsten fügen Sie aber ein Abbild und alle zugehörigen Installationsdateien aus dem Installationsmedium hinzu. Diese Schritte arbeiten Sie in den Übungen weiter unten in dieser Lektion durch. Das bietet Flexibilität, weil eine einzige *Install.wim*-Datei Abbilder für mehrere Windows 7-Editionen enthalten kann. Der Ansatz arbeitet mit einem Thin-Abbild, weil die Abbilder auf dem Installationsmedium keine Treiber anderer Hersteller, Windows Installer-Dateien, wichtige Anwendungen oder zusätzliche Language Packs enthalten. Vor allem fehlen aber die kritischen Sicherheitsupdates, die veröffentlicht wurden, seit das Installationsabbild erstellt wurde. Wenn Sie solche Abbilder auf mehrere Clientcomputer anwenden und diese Computer online bringen, bedeutet das ein Sicherheitsrisiko, sofern nicht zumindest die kritischen Sicherheitsupdates vor der Bereitstellung zum Abbild hinzugefügt werden.

Um Abbilder mit MDT 2010 bereitzustellen, müssen Sie das Quellverzeichnis angeben, in dem die WIM-Datei liegt. Der Assistent zum Importieren von Betriebssystemen verschiebt die Datei in die Bereitstellungsfreigabe. Um ein Betriebssystemabbild zur Bereitstellungsfreigabe hinzuzufügen, gehen Sie folgendermaßen vor:

1. Erweitern Sie in der Konsolenstruktur der Deployment Workbench unter dem Knoten *Deployment Shares* den Knoten Ihrer Bereitstellungsfreigabe, klicken Sie mit der rechten Maustaste auf *Operating Systems* und wählen Sie den Befehl *Import Operating System* (oder klicken Sie auf *Operating Systems* und dann im Fensterabschnitt *Aktionen* auf *Import Operating System*). Daraufhin wird der Assistent zum Importieren von Betriebssystemen (*Import Operating System Wizard*) gestartet.

2. Wählen Sie auf der Seite *OS Type* den Typ des Abbilds aus (benutzerdefiniert, Installationsdateien oder WDS), das Sie hinzufügen wollen.
3. Wählen Sie eine Abbildquelle aus und geben Sie den Zielordner an, der ein Unterordner der Bereitstellungsfreigabe sein muss. Wenn es sich um ein benutzerdefiniertes Abbild handelt, haben Sie die Möglichkeit, die Dateien in die Bereitstellungsfreigabe zu verschieben, statt sie dorthin zu kopieren.

Hinzufügen von Gerätetreibern

Sobald das Betriebssystem zur Deployment Workbench hinzugefügt wurde, können Sie auch die benötigten Gerätetreiber hinzufügen. Während der Bereitstellung des Betriebssystems werden diese Treiber zu Windows PE und den Zielcomputern hinzugefügt, sodass sie mit Windows 7 bereitgestellt werden. Der Assistent zum Importieren von Treibern in der Deployment Workbench kopiert die Gerätetreiberdateien in die Bereitstellungsfreigabe. Sie gehen folgendermaßen vor, um Out-of-Box-Gerätetreiber (Treiber anderer Hersteller) hinzufügen:

1. Erweitern Sie in der Konsolenstruktur der Deployment Workbench unter dem Knoten *Deployment Shares* den Knoten Ihrer Bereitstellungsfreigabe, wählen Sie den Knoten *Out-of-Box Drivers* aus und klicken Sie im Fensterabschnitt *Aktionen* auf *Import Drivers*.

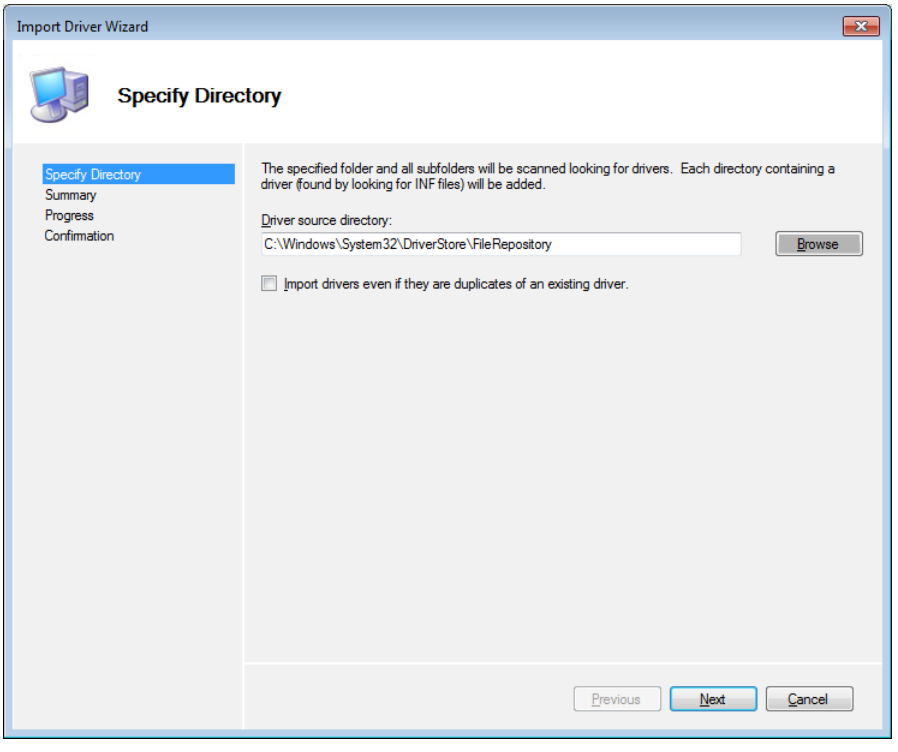


Abbildung 3.21 Angeben des Pfads für Treiberdateien

2. Geben Sie im Assistenten zum Importieren von Treibern (*Import Driver Wizard*) den Pfad des Ordners ein, in dem die Treiber liegen, die Sie hinzufügen wollen. Abbildung 3.21 zeigt, wie der Pfad eines Ordners eingegeben wird, auf dem Treiber im

Computer *Canberra* gespeichert sind. In der Praxis erstellen Sie allerdings eher einen speziellen Ordner, in dem Sie alle Treiber anderer Hersteller speichern, die Sie installieren wollen.

3. Gehen Sie die restlichen Seiten des Assistenten durch, um die Treiber zu importieren.
4. Klicken Sie auf *Finish*, um den Assistenten zu schließen.

Die Out-of-Box-Gerätetreiber werden in Unterordnern des Ordners *C:\Distribution\Out-of-Box Drivers* installiert.

Konfigurieren von Tasksequenzen

Tasksequenzen verwenden Sie, um Updates, Language Packs und andere Pakete sowie Anwendungen zu einem Abbild hinzuzufügen. Außerdem geben Sie eine Tasksequenz an, die Quelldateien des Betriebssystems mit einer Konfiguration verknüpft. Zu den Quelldateien des Betriebssystems gehören:

- **Betriebssystem** Sie können ein Betriebssystem oder ein benutzerdefiniertes Abbild auswählen, das für den Build verwendet wird.
- **Antwortdatei für unbeaufsichtigtes Setup (*Unattend.xml* oder *Autounattend.xml*)** Sie können eine Antwortdatei erstellen, die beschreibt, wie Windows 7 auf dem Zielcomputer installiert und konfiguriert wird. Die Antwortdatei enthält beispielsweise den Product Key, den Organisationsnamen und Informationen, die gebraucht werden, um den Computer zu einer Domäne hinzuzufügen. Kapitel 2 hat beschrieben, wie Sie Antwortdateien für die unbeaufsichtigte Installation mithilfe von Windows SIM erstellen.
- **Tasksequenz** Jeder Build hat eine Standardtasksequenz für die unbeaufsichtigte Installation.

Erstellen und Bearbeiten einer Tasksequenz

Das Tasksequenzmodul (task sequencer) führt die Tasksequenz in der angegebenen Reihenfolge aus. Jede Task in der Sequenz ist ein Schritt, und diese Schritte können in Gruppen und Untergruppen zusammengefasst werden. Wenn Sie eine Tasksequenz in der Deployment Workbench erstellen, legt das Tool eine Standardtasksequenz an. Sie haben die Möglichkeit, Tasks und Gruppen zu bearbeiten. Außerdem können Sie Tasksequenzen importieren, die von anderen Softwarepaketen erstellt wurden, etwa SCCM 2007.

Tasksequenzen enthalten folgende Elementtypen:

- **Tasks** Innerhalb einer Tasksequenz sind Tasks die Befehle, die das Tasksequenzmodul während der Sequenz ausführt, um beispielsweise die Festplatte zu partitionieren, den Benutzerstatus aufzuzeichnen und das Betriebssystem zu installieren. In der Standardtasksequenz sind die meisten Tasks Befehle, die Skripts ausführen.
- **Gruppen (group)** Tasksequenzen können in Gruppen zusammengefasst werden. Eine solche Gruppe ist ein Ordner, der Untergruppen und Tasks enthält. Zum Beispiel fasst die Standardtasksequenz Tasks in Gruppen zusammen, die den unterschiedlichen Phasen und Bereitstellungstypen entsprechen. Tasks und Gruppen (inklusive der Gruppen und Tasks, die sie enthalten) können anhand der angegebenen Bedingungen gefiltert werden. Gruppen sind nützlich bei der Filterung, weil die Ausführung einer ganzen Reihe von Tasks veranlasst werden kann, die eine bestimmte Bedingung erfüllen, zum Beispiel alle Tasks für eine bestimmte Bereitstellungsphase oder einen Bereitstellungstyp.

Sie erstellen Tasksequenzen mit dem integrierten Editor der Deployment Workbench. Jede Tasksequenz besteht aus einer Abfolge von Schritten, die zusammen eine bestimmten Task bilden. Tasksequenzen können sich über den Neustart eines Computers erstrecken, meist werden sie so entworfen, dass sie die Ausführung von Aufgaben auf einem Computer automatisieren, ohne dass der Benutzer eingreifen muss. Tasksequenzschritte können zu einer Tasksequenzgruppe hinzugefügt werden. Auf diese Weise werden verwandte Tasksequenzschritte zusammengefasst, sodass sie übersichtlicher organisiert sind und Fehler einfacher beseitigt werden können.

Tasksequenzschritte können Tools und Skripts aufrufen, die zusammen mit MDT 2010 zur Verfügung gestellt oder als benutzerdefinierte Lösungen für eine bestimmte Aufgabe entwickelt werden. Im Tasksequenz-Editor definieren Sie die Tasksequenzgruppen, Tasksequenzschritte und die gültigen Eigenschaften und Optionen, um alle Abschnitte des Abbildvorbereitungs- und Bereitstellungsprozesses zu steuern. Für jede Tasksequenzgruppe und jeden Schritt müssen Sie folgende Informationen angeben:

- **Name** Der Name der Tasksequenzgruppe oder des Tasksequenzschritts
- **Beschreibung** Beschreibt den Zweck der Tasksequenzgruppe oder des Tasksequenzschritts und liefert Informationen über seine Anpassung.
- **Eigenschaften** Gibt die Konfigurationseigenschaften für die Tasksequenzgruppe oder den Tasksequenzschritt an und definiert, wie die Task ausgeführt wird.
- **Optionen** Gibt die Konfigurationsoptionen an, die für die Tasksequenzgruppe oder den Tasksequenzschritt eingestellt werden können, wenn die Task ausgeführt wird. Definiert außerdem die Bedingungen für einen erfolgreichen Abschluss.



Hinweis Zusätzliche Typen für Tasksequenzschritte

Wenn Sie Tasksequenzen mit SCCM 2007 konfigurieren, stehen normalerweise weitere Tasksequenzschritttypen und bedingte Anweisungen zur Verfügung.

Sie gehen folgendermaßen vor, wenn Sie eine Tasksequenz in MDT 2010 erstellen:

1. Wählen Sie in der Deployment Workbench den Unterknoten *Task Sequences* aus und klicken Sie im Fensterabschnitt *Aktionen* auf *New Task Sequence*. Geben Sie auf der Seite *General Settings* des Assistenten für neue Tasksequenzen (*New Task Sequence Wizard*) eine ID und einen Namen für die Tasksequenz ein. Bei Bedarf können Sie auch einen Kommentar hinzufügen.
2. Wählen Sie auf der Seite *Select Template* eine Vorlage für die Tasksequenz aus der Liste (Abbildung 3.22).
3. Wählen Sie auf der Seite *Select OS* ein Betriebssystem aus, das Sie mit der Tasksequenz verknüpfen wollen. Dabei stehen nur die Betriebssysteme aus dem WIM-Abbild zur Auswahl, das Sie in der Bereitstellungsfreigabe hinzugefügt haben.
4. Auf der Seite *Specify Product Key* können Sie einen Product Key angeben oder die Eingabe dieser Daten bis zur Bereitstellung aufschieben.
5. Geben Sie auf der Seite *OS Settings* Ihren vollständigen Namen, Ihre Organisation und die Internet Explorer-Startseite Ihrer Organisation ein.

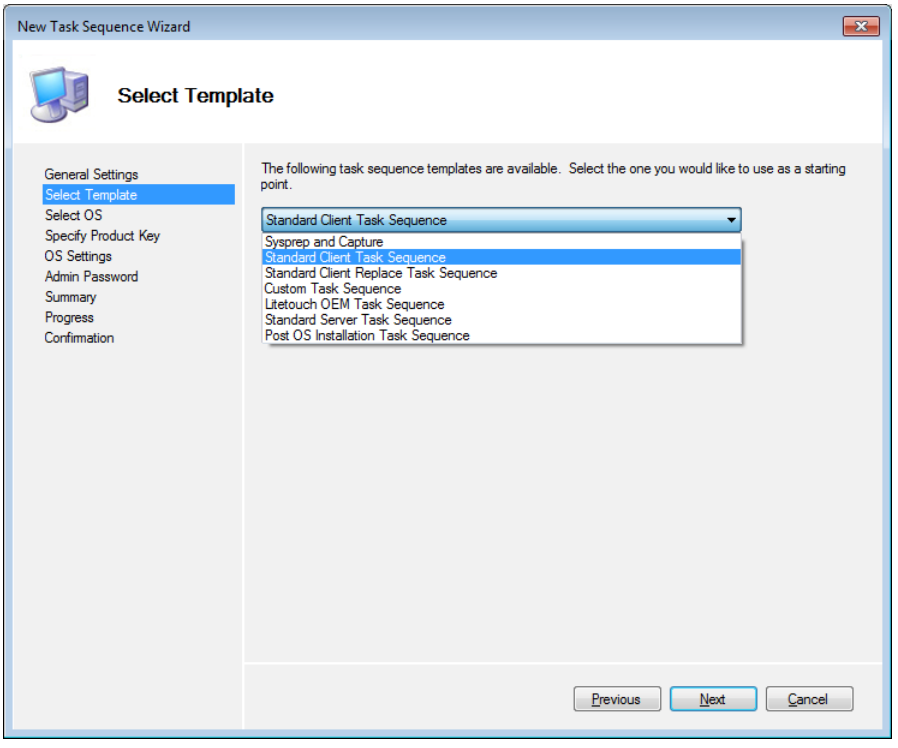


Abbildung 3.22 Verfügbare Vorlagen für Tasksequenzen

6. Auf der Seite *Admin Password* haben Sie die Wahl, ein Administratorkennwort einzugeben und zu bestätigen oder die Eingabe des Kennworts bis zur Bereitstellung aufzuschieben.
7. Prüfen Sie Ihre Einstellungen auf der Seite *Summary* und klicken Sie auf *Next*, um die Tasksequenz zu generieren.
8. Klicken Sie auf *Finish*, um den Assistenten zu schließen. Die Tasksequenz wird nun in der Deployment Workbench aufgelistet (Abbildung 3.23).
9. Sie bearbeiten die Tasksequenz, indem Sie den Eintrag mit der rechten Maustaste anklicken und den Befehl *Eigenschaften* wählen. Auf der Registerkarte *General* können Sie Einstellungen wie den Namen der Tasksequenz ändern. Außerdem können Sie festlegen, auf welche Clientbetriebssysteme die Tasksequenz angewendet wird (Abbildung 3.24).
10. Die Registerkarte *Task Sequence* einer neuen Tasksequenz zeigt die Vorlage, die Sie für Ihre Tasksequenz ausgewählt haben. Abbildung 3.25 zeigt die Vorlage *Standard Client Task Sequence*. Sie können diese Vorlage anpassen, damit Ihre neue Tasksequenz die benötigten Tasks ausführt (normalerweise löschen Sie dabei die nicht benötigten Tasks). Auf der Registerkarte *Options* innerhalb der Registerkarte *Task Sequence* können Sie den Schritt deaktivieren, festlegen, ob die Task auch beim Auftreten eines Fehlers fortgesetzt wird, und (in manchen Fällen) die Rückgabewerte für eine erfolgreiche Ausführung eintragen.

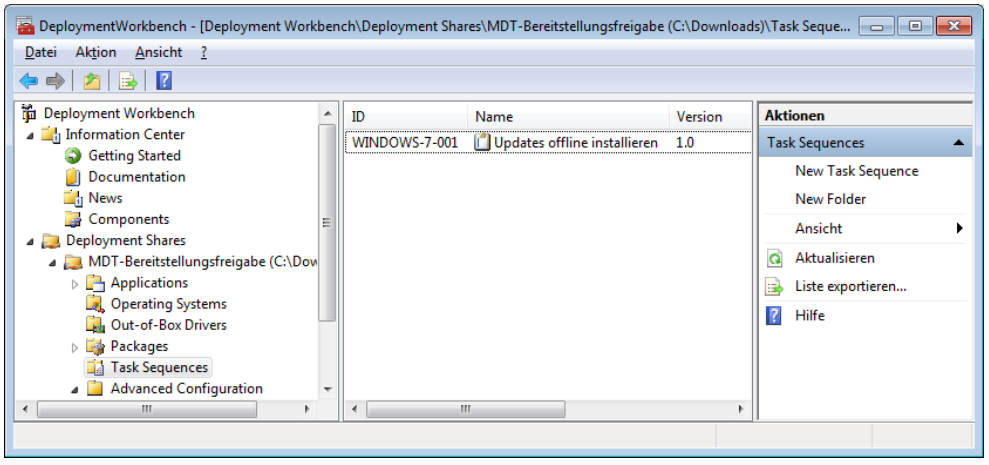


Abbildung 3.23 Eine Tasksequenz in der Deployment Workbench

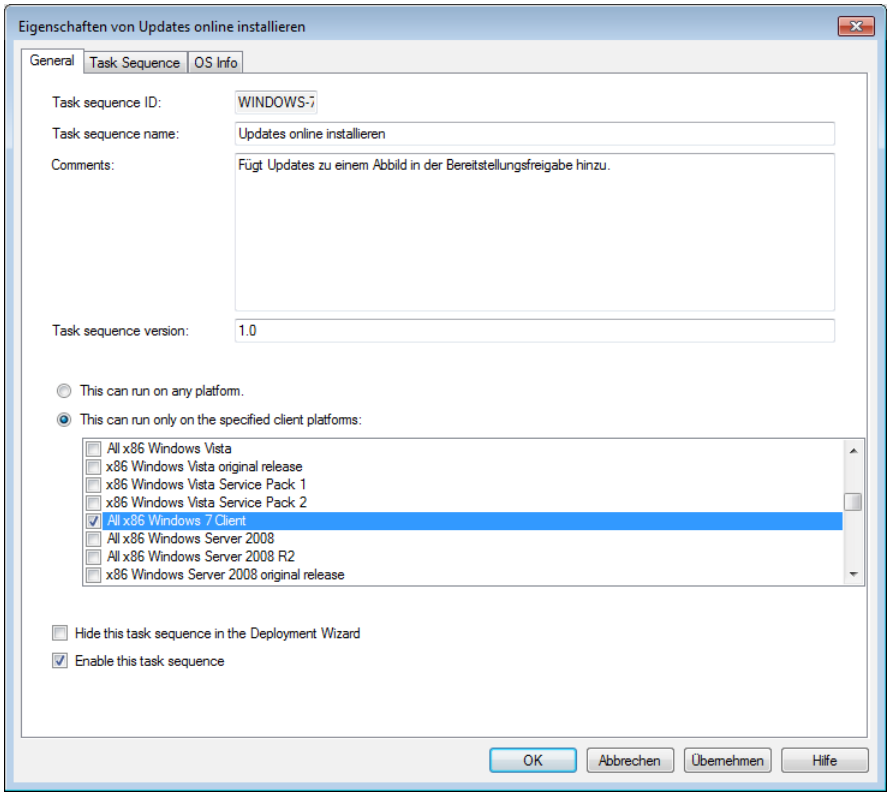


Abbildung 3.24 Bearbeiten der Tasksequenzeigenschaften auf der Registerkarte *General*

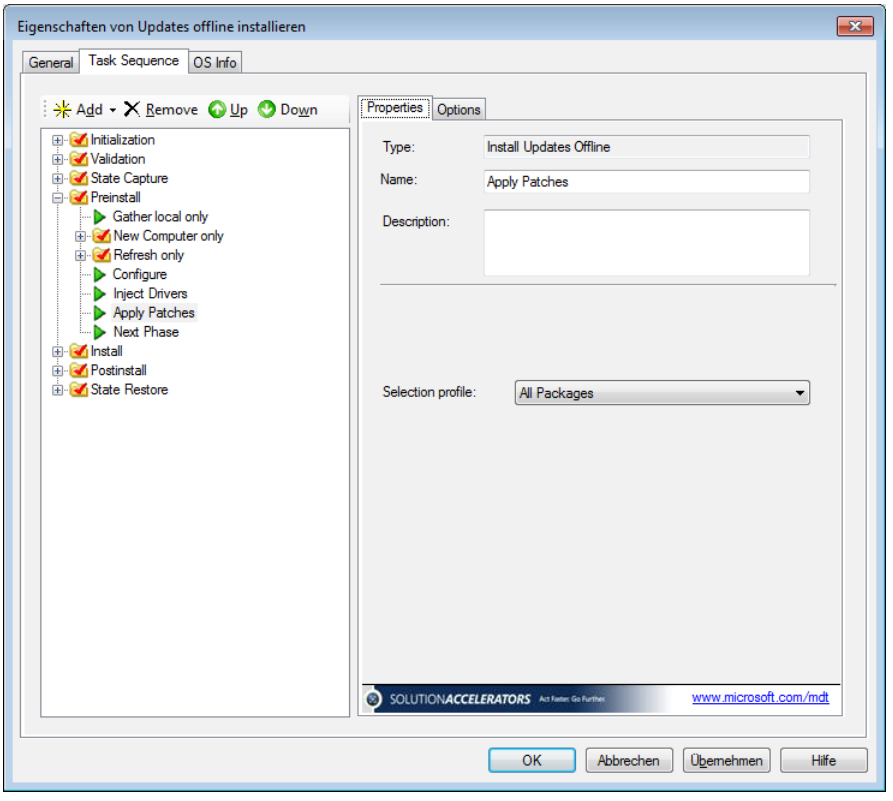


Abbildung 3.25 Die Vorlage *Standard Client Task Sequence*



Weitere Informationen Tasksequenz-Editor

Weitere Informationen über den Tasksequenz-Editor finden Sie in *Betriebssystembereitstellung: Tasksequenz-Editor* unter *http://technet.microsoft.com/de-de/library/bb680396.aspx*.

Erstellen einer Tasksequenz zum Bereitstellen von Windows 7 auf einer VHD

Gelegentlich müssen Sie ein Windows 7-Abbild bereitstellen, mit dem Ihre Clientcomputer von VHD starten können. Möglicherweise arbeiten einige Benutzer noch mit Windows Vista und möchten in einer Dual-Boot-Konfiguration Windows 7 ausprobieren, bevor sie endgültig umsteigen. Für diesen Zweck können Sie virtuelle Windows 7-Computer auf den Clientcomputern erstellen. Allerdings ist es nicht ganz simpel, das über eine zentralisierte Bereitstellung zu erledigen.

Eine zweite Möglichkeit besteht darin, mit MDT 2010 auf jedem Clientcomputer Windows 7 in einer startfähigen VHD bereitzustellen. Die Benutzer können dann auswählen, ob sie Windows Vista oder Windows 7 (von der VHD) starten. Das ist eine komfortable Möglichkeit für Clientcomputer, die nur eine einzige Festplatte haben. Denn auf diese Weise brauchen Sie die Partitionierung des Laufwerks nicht für Windows 7 umzustellen und können die ursprünglichen Betriebssysteme unverändert lassen.

In der Standardeinstellung stellt MDT 2010 Windows 7 in Partition 1 von Datenträger 0 bereit. Um dieses Verhalten so zu ändern, dass MDT 2010 die Bereitstellung in einer VHD

durchführt und das vorhandene Betriebssystem nicht antastet, müssen Sie eine Standardtasksequenz erstellen, die Windows 7 installiert, und sie dann folgendermaßen ändern:

1. Erweitern Sie auf der Registerkarte *Task Sequence* im Eigenschaftendialogfeld der Tasksequenz die Knoten *Preinstall* sowie *New Computer Only* und klicken Sie auf *Format and Partition Disk*.
2. Deaktivieren Sie diesen Schritt (Abbildung 3.26).

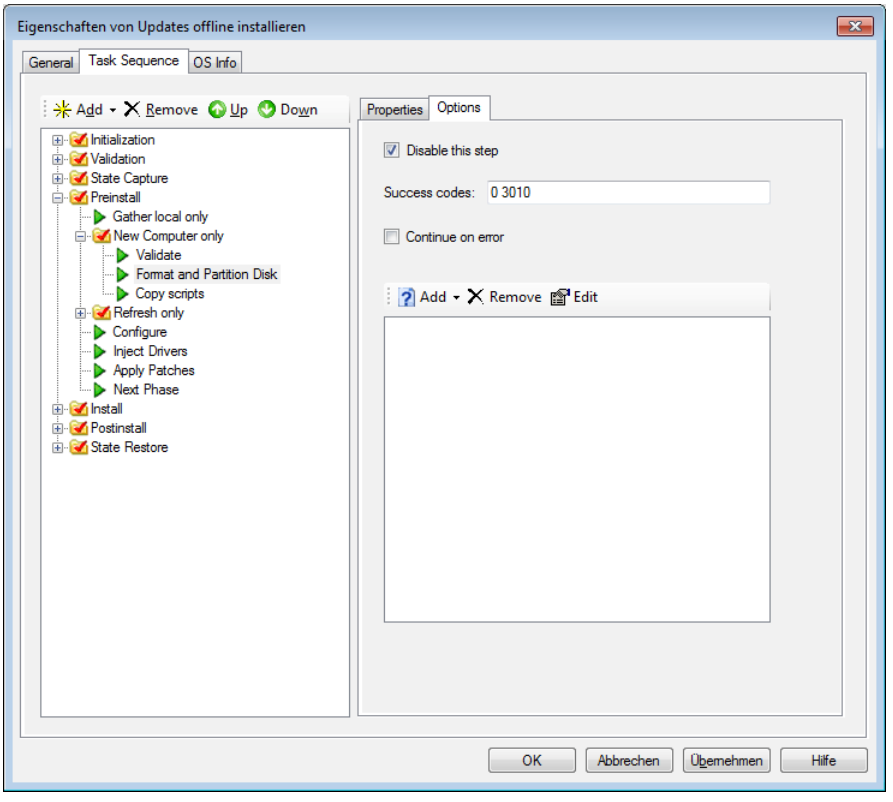


Abbildung 3.26 Deaktivieren des Schritts *Format and Partition Disk*

3. Klicken Sie links oben auf der Registerkarte *Task Sequence* auf *Add* und wählen Sie die Menüeinträge *General* und dann *Set Task Sequence Variable*. Konfigurieren Sie die Tasksequenzvariable `BootVHDLocation` wie in Abbildung 3.27 gezeigt.
4. Klicken Sie erneut links oben auf *Add* und wählen Sie die Menüeinträge *General* und dann *Set Task Sequence Variable*. Konfigurieren Sie die Tasksequenzvariable `BootVHDSize` wie in Abbildung 3.28 gezeigt. Stellen Sie sicher, dass genug Platz (20 GByte) auf dem Laufwerk frei ist, weil die VHD bis zu dieser Größe wachsen kann.
5. Klicken Sie links oben auf *Add* und wählen Sie die Menüeinträge *General* und dann *Run Command Line*. Geben Sie dem Element den Namen *VHD einrichten*. Tragen Sie die Befehlszeile `cscript.exe "%ScriptRoot%\ZTIDiskPartVHD.wsf"` ein (Abbildung 3.29).
6. Klicken Sie auf *Übernehmen*.

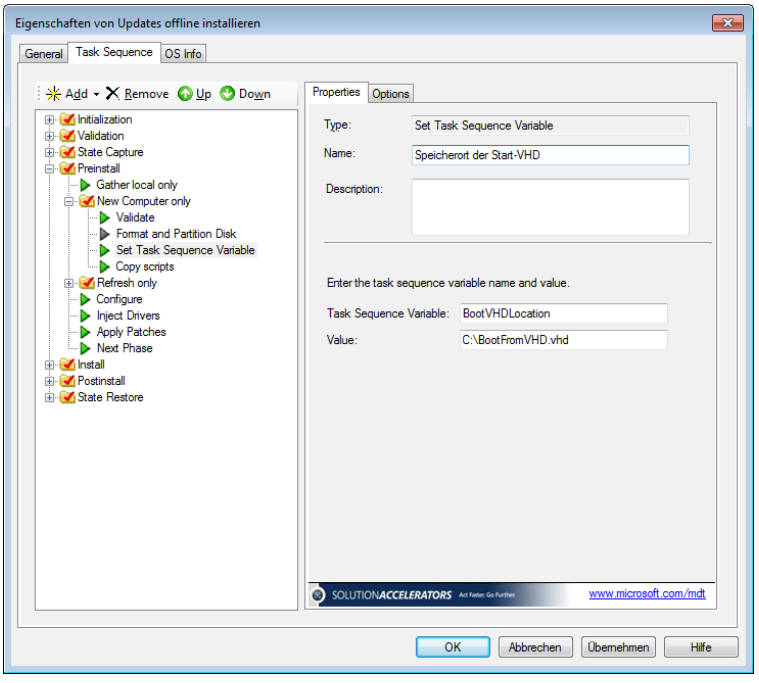


Abbildung 3.27 Konfigurieren der Variablen `BootVHDLocation`

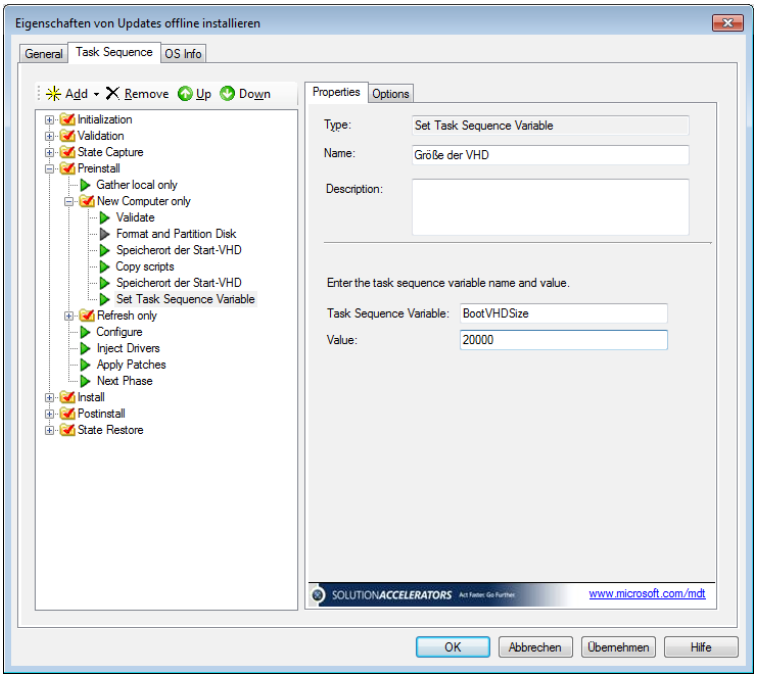


Abbildung 3.28 Konfigurieren der Größe der VHD

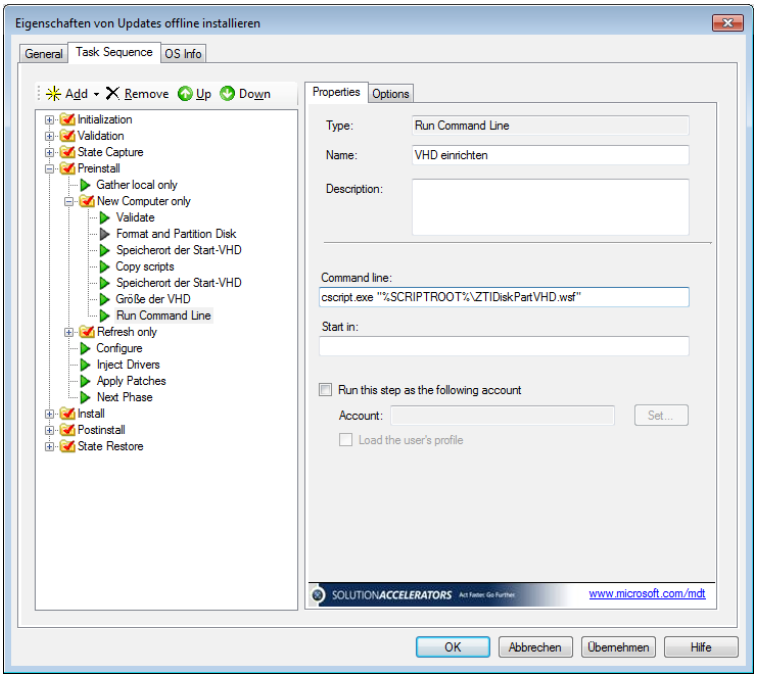


Abbildung 3.29 Einfügen einer Befehlszeile

Mithilfe dieser Tasksequenz wird Windows 7 in einer VHD bereitgestellt statt auf der internen Festplatte.

Hinzufügen von Updates

Wenn Sie ein Abbild entwickeln, sollten Sie sicherstellen, dass alle kritischen Sicherheitsupdates darin enthalten sind. Sie haben unterschiedliche Ansätze zur Auswahl, um diese Updates einzuspielen. Microsoft empfiehlt, dass Sie die Updates nach Möglichkeit offline einspielen. Für diese Aufgabe stehen folgende Verfahren zur Verfügung (sofern eine Bereitstellungsfreigabe vorhanden ist):

- **Updates offline hinzufügen** Mit MDT 2010 können Sie Updates offline mithilfe einer Tasksequenz installieren. Wählen Sie dazu im Tasksequenz-Editor der Deployment Workbench die Task *Install Updates Offline* aus. Diese Möglichkeit wird nur angeboten, wenn SCCM 2007 in Ihrem Netzwerk verfügbar ist.
- **Updates online hinzufügen** Sie können mit MDT 2010 Updates online installieren, indem Sie eine Tasksequenz einsetzen. Wählen Sie dazu im Tasksequenz-Editor der Deployment Workbench die Task *Install Updates Online* aus. Wie bei der Offlinevariante wird auch hier vorausgesetzt, dass SCCM 2007 in Ihrem Netzwerk verfügbar ist.
- **Hinzufügen von Updates zum Masterabbild** Sie können Sicherheitsupdates von der Microsoft Update-Website herunterladen und dann im Rahmen des Abbilderstellungsprozesses installieren, wenn Sie ein benutzerdefiniertes Abbild anwenden. Zusätzliche Updates fügen Sie hinzu, indem Sie die heruntergeladenen Updates in die Bereitstellungsfreigabe legen. Sie können Updates zu einem Installationsabbild hinzufügen, das Sie vom Installationsmedium kopiert haben, indem Sie sie aus dem Microsoft Update-Katalog unter *http://catalog.update.microsoft.com/v7/site/Home.aspx*

herunterladen und in einer Bereitstellungsfreigabe speichern. Abbildung 3.30 zeigt die Startseite des Microsoft Update-Katalogs.

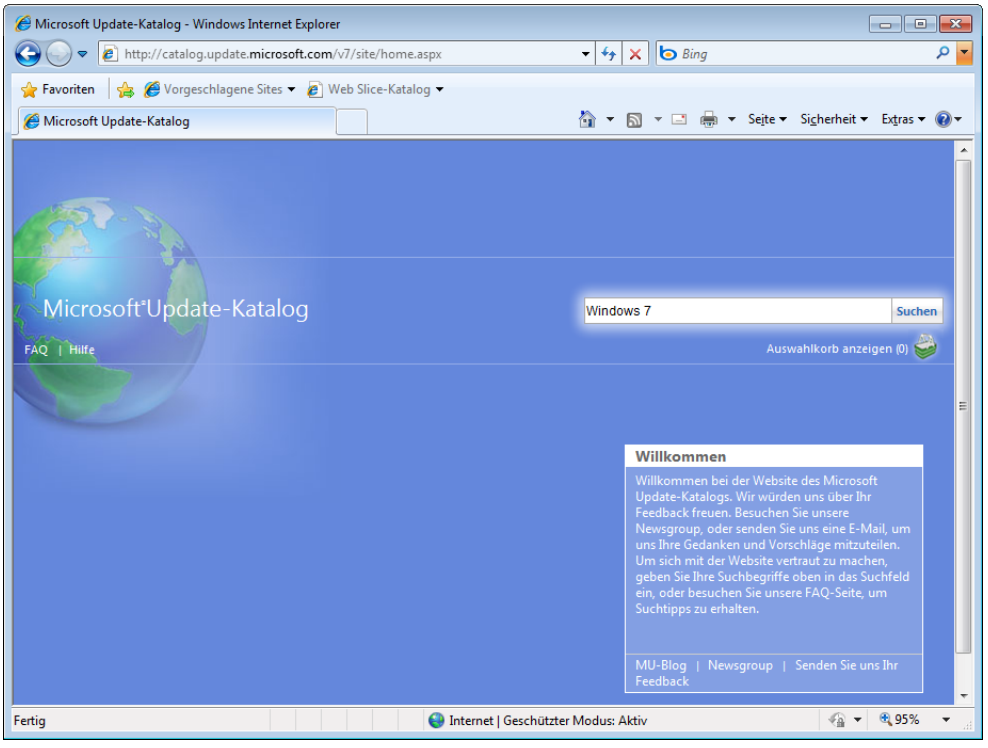

Microsoft Update-Katalog - Windows Internet Explorer
http://catalog.update.microsoft.com/v7/site/home.aspx
Bing
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Microsoft Update-Katalog
Seite
Sicherheit
Extras
Microsoft Update-Katalog
FAQ | Hilfe
Windows 7
Suchen
Auswahlkorb anzeigen (0)
Willkommen
Willkommen bei der Website des Microsoft Update-Katalogs. Wir würden uns über Ihr Feedback freuen. Besuchen Sie unsere Newsgroup, oder senden Sie uns eine E-Mail, um uns Ihre Gedanken und Vorschläge mitzuteilen. Um sich mit der Website vertraut zu machen, geben Sie Ihre Suchbegriffe oben in das Suchfeld ein, oder besuchen Sie unsere FAQ-Seite, um Suchtipps zu erhalten.
MU-Blog | Newsgroup | Senden Sie uns Ihr Feedback
Fertig
Internet | Geschützter Modus: Aktiv
95%

Abbildung 3.30 Die Startseite des Microsoft Update-Katalogs

- **Hinzufügen von Updates mit WSUS oder SCCM 2007** Sie können WSUS oder SCCM 2007 einsetzen, um die Sicherheitsupdates nach der Bereitstellung zu installieren. Abhängig von der Konfiguration dauert es unter Umständen über 1 Stunde, bis alle Updates angewendet worden sind. Wenn Sie den SCCM-Client in das Abbild aufnehmen und ihn so einstellen, dass er mit einer bestimmten SCCM-Site kommuniziert, stellen Sie sicher, dass alle Computer, die auf Basis dieses Abbilds eingerichtet werden, nur mit dieser eingestellten Site kommunizieren.
- **Slipstreamupdates in der Installationsquelle** Sie können Sicherheitsupdates aus dem Microsoft Update-Katalog herunterladen und in die Windows-Installationsquelle integrieren, bevor Sie den unbeaufsichtigten Buildprozess anstoßen. Auf diese Weise ist das Abbild vor bekannten Sicherheitslücken geschützt, aber es erfordert Verwaltungsaufwand, die Sicherheitsupdates zu integrieren.

Eine Offlinedatei auf einer VHD auf dem neusten Stand halten

Mit dem Offline Virtual Machine Servicing Tool, das in Kapitel 2 beschrieben wurde, können Sie VHD-Offlinedateien, die Installationen von Windows 7 enthalten, mit Service Packs und Softwareupdates auf dem neusten Stand halten. Das Offline Virtual Machine Servicing Tool ist in der Lage, sehr viele virtuelle Computer oder VHDs, die meist offline sind, entsprechend den individuellen Anforderungen zu aktualisieren. Das Tool arbeitet mit SCVMM

2007 oder SCVMM 2008 zusammen, außerdem kann es auf WSUS 3.0, SCCM 2007 oder Configuration Manager 2007 R2 zugreifen.

Das Tool arbeitet mit dem Konzept von »Wartungsaufträgen« (servicing job), um die Updateoperationen anhand von Listen aller vorhandenen virtuellen Computer zu verwalten, die in SCVVM gespeichert sind. Ein Wartungsauftrag führt Windows PowerShell-Skripts aus, um auf die virtuellen Computer und VHDs zuzugreifen. Der Wartungsauftrag stellt dabei einen virtuellen Computer auf einem Host bereit und startet ihn, oder er startet einen Computer, auf dem für Failoverzwecke ein Abbild installiert ist, von diesem Abbild, stößt den Softwareupdatezyklus an und schließt das aktualisierte Gerät wieder. Zuletzt fährt das Offline Virtual Machine Servicing Tool entweder den virtuellen Computer herunter oder startet den Computer, auf dem die VHD installiert ist, von seinem normalen Startabbild neu.

Wenn Sie dieses Tool verwenden, konfigurieren Sie Gruppen aus virtuellen Computern (oder VHDs) und erstellen Wartungsaufträge, für die Sie anschließend einen Zeitplan festlegen. Sie können Aufträge so planen, dass sie sofort ausgeführt werden oder nur während eines Wartungsfensters, in dem wenig Netzwerkverkehr stattfindet. Außerdem können Sie Wartungsaufträge so planen, dass sie in regelmäßigen Abständen ausgeführt werden. Der Nachteil des Offline Virtual Machine Servicing Tools besteht darin, dass ein virtueller oder ein physischer Computer mit startfähiger VHD in unsicherem Zustand online gebracht wird (wenn auch nur für kurze Zeit), damit das Abbild aktualisiert werden kann.



Weitere Informationen Offline Virtual Machine Servicing Tool und SCVMM

Weitere Informationen über das Offline Virtual Machine Servicing Tool finden Sie unter *http://technet.microsoft.com/en-us/library/cc501231.aspx*. Weitere Informationen über SCVMM 2008 enthält die Seite *http://technet.microsoft.com/en-us/library/cc668737.aspx*; wählen Sie dort die gewünschten Links im Navigationsabschnitt aus.

Hinzufügen von Language Packs

Language Packs richten eine mehrsprachige Windows-Umgebung ein. Windows-Betriebssysteme sind sprachneutral. Sprach- und Gebietsschemaressourcen werden über Language Packs (*lp.cab*-Dateien) hinzugefügt. Sobald Sie ein oder mehrere Language Packs zu Windows 7 hinzugefügt haben, können Sie die entsprechenden Sprachen auswählen, wenn Sie das Betriebssystem installieren. Daher kann dasselbe Windows 7-Abbild in Gebieten mit unterschiedlichen Sprachen und Regionseinstellungen bereitgestellt werden, was Entwicklungs- und Bereitstellungsdauer verkürzt.

Sie können Language Packs offline oder online mit MDT 2010 und SCCM 2007 hinzufügen. Wählen Sie dazu im Tasksequenz-Editor der Deployment Workbench die Task *Install Language Packs Offline* beziehungsweise *Install Language Packs Online* aus. Sie bekommen daraufhin eine Liste der Language Packs angeboten, die Sie hinzufügen können. Falls SCCM 2007 nicht verfügbar ist, können Sie Language Packs über eine benutzerdefinierte Tasksequenz hinzufügen, indem Sie eine Vorlage auswählen, die die Schritte zum Hinzufügen von Paketen enthält.

Hinzufügen von Anwendungen

Wenn Sie einen Referenzcomputer benutzen, können Sie Anwendungen auf diesem Computer installieren und dann ein Abbild aufzeichnen. Passen Sie auf, dass Sie nicht gegen die Lizenzbedingungen verstoßen, wenn Sie das Abbild auf anderen Computern installieren.

Sie können Anwendungen auch zu einem vorhandenen Abbild hinzufügen, indem Sie sie in die Bereitstellungsfreigabe legen. Die Deployment Workbench ist in der Lage, die Anwendung aus dem ursprünglichen Netzwerkstandort zu installieren oder die Quelldateien der Anwendung in die Bereitstellungsfreigabe zu kopieren. In beiden Fällen können Sie die Befehle zum Installieren der Anwendung angeben, wenn Sie sie zur Bereitstellungsfreigabe hinzufügen. Anwendungen können auch im Rahmen von ZTI-Bereitstellungen als SCCM 2007-Pakete installiert werden. Sobald Sie eine Anwendung zur Bereitstellungsfreigabe hinzugefügt haben, haben Sie folgende Möglichkeiten, sie zu installieren:

- **Hinzufügen der Anwendung zur Tasksequenz** Anwendungen, die zur Tasksequenz hinzugefügt wurden, werden installiert, sobald MDT 2010 die Tasksequenz auf dem Zielcomputer ausführt. Bei der OEM-Anwendung eines anderen Herstellers verwenden Sie üblicherweise die Vorlage *Litetouch OEM Task Sequence* und konfigurieren den Schritt *Copy Media CD to Local Hard Disk for OEM pre-installation*.
- **Verwenden des Assistenten für neue Anwendungen** Sie starten diesen Assistenten (New Application Wizard), indem Sie den Knoten Ihrer Bereitstellungsfreigabe erweitern, mit der rechten Maustaste auf *Applications* klicken und im Kontextmenü den Befehl *New Application* wählen. Abbildung 3.31 zeigt die Seite *Application Type* des Assistenten. Auf den weiteren Seiten des Assistenten geben Sie Name und Herausgeber der Anwendung an, wählen das Quellverzeichnis für die Anwendungsdateien aus, legen fest, ob Sie diese Dateien verschieben oder kopieren wollen, tragen den Namen des Zielverzeichnisses ein und geben die Befehlszeile ein, mit der die Anwendung installiert wird.

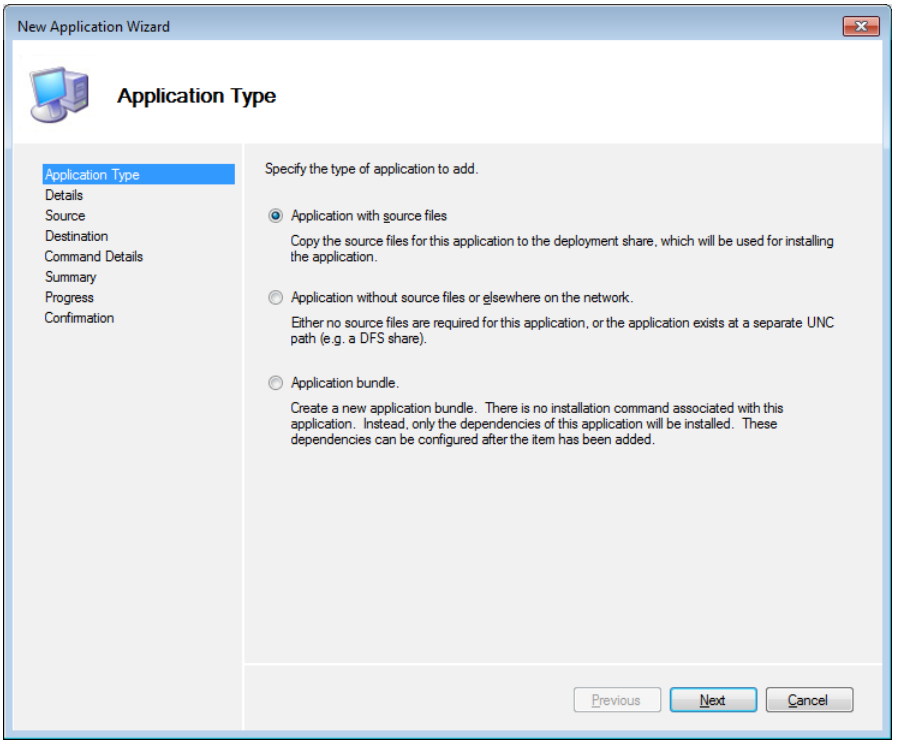

New Application Wizard
Application Type
Application Type
Details
Source
Destination
Command Details
Summary
Progress
Confirmation
Specify the type of application to add.
Application with source files
Copy the source files for this application to the deployment share, which will be used for installing the application.
Application without source files or elsewhere on the network.
Either no source files are required for this application, or the application exists at a separate UNC path (e.g. a DFS share).
Application bundle.
Create a new application bundle. There is no installation command associated with this application. Instead, only the dependencies of this application will be installed. These dependencies can be configured after the item has been added.
Previous
Next
Cancel

Abbildung 3.31 Der Assistent für neue Anwendungen



Vorsicht Erlauben Sie einer Anwendung nicht, den Computer neu zu starten

Wenn Sie MDT 2010 benutzen, dürfen Sie einer Anwendung nicht erlauben, den Computer neu zu starten. MDT 2010 muss selbst steuern, wann der Computer neu gestartet wird, sonst schlägt die Tasksequenz fehl. Mithilfe der Befehlszeileneigenschaft `reboot=reallysuppress` können Sie verhindern, dass Anwendungen einen Neustart durchführen.



Prüfungstipp

Sie können eine Anwendung nicht mit DISM zu einem Abbild hinzufügen. Allerdings ist es möglich, eine Anwendung in einer Bereitstellungsfreigabe von MDT 2010 zu einem Abbild hinzuzufügen.



Hinweis Konfigurieren einer Bereitstellungsdatenbank

Mit dem Assistenten für eine neue Datenbank in der Deployment Workbench können Sie eine Bereitstellungsdatenbank konfigurieren. Dafür brauchen Sie in Ihrem Netzwerk einen Server, der SQL Server 2005 oder SQL Server 2008 ausführt. Diese Funktion wird genutzt, wenn MDT 2010 mit SCCM 2007 zusammenarbeitet.

Konfigurieren von Windows PE-Optionen

Nachdem Sie eine Bereitstellungsfreigabe erstellt haben, können Sie ihre Windows PE-Konfigurationsoptionen bearbeiten. Nehmen wir an, Sie haben eine Bereitstellungsfreigabe namens *Testumgebung* angelegt. Führen Sie nun in der Deployment Workbench folgende Schritte aus:

1. Wählen Sie in der Konsolenstruktur der Deployment Workbench den Knoten der *Deployment Shares* aus.
2. Klicken Sie in der Detailansicht mit der rechten Maustaste auf *Testumgebung* und wählen Sie im Kontextmenü den Befehl *Eigenschaften*.
3. Aktivieren Sie im Dialogfeld *Eigenschaften von Testumgebung* die Registerkarte *Windows PE x86 Components*.
4. Wählen Sie im Feld *Driver Injection* die Gerätetreibergruppe aus, die Sie vorher im Bereitstellungsprozess erstellt haben (zum Beispiel *Windows 7*), und klicken Sie auf *OK*.
5. Klicken Sie in der Detailansicht mit der rechten Maustaste auf *Testumgebung* und wählen Sie den Befehl *Aktualisieren*.

Daraufhin wird die Bereitstellungsfreigabe aktualisiert, sodass sie ein Windows PE-Verzeichnis anlegt. Alle MDT 2010-Konfigurationsdateien werden aktualisiert, und die Deployment Workbench generiert eine angepasste Windows PE-Version, die Sie anschließend verwenden, um den LTI-Bereitstellungsprozess zu starten.

Die Deployment Workbench erstellt die Dateien *LiteTouchPE_x86.iso* und *LiteTouchPE_x86.wim* (für 32-Bit-Zielcomputer) im Ordner *C:\Distribution\Boot* (wobei *C:\Distribution* der freigegebene Ordner ist, der als Bereitstellungsfreigabe benutzt wird).

Erstellen von startfähigen LTI-Medien

Wenn Sie einen Referenzcomputer starten und ein Abbild für die Verteilung aufzeichnen wollen, müssen Sie ein startfähiges Medium erstellen, das die angepasste Windows PE-Version enthält, die Sie beim Aktualisieren der Bereitstellungsfreigabe erstellt haben. Sie können ein geeignetes startfähiges LTI-Medium aus der Datei *LiteTouchPE_x86.iso* oder *LiteTouchPE_x86.wim* erstellen. Falls der Referenzcomputer ein physischer Computer ist, können Sie aus der ISO-Datei eine startfähige DVD brennen. Handelt es sich um einen physischen Computer mit startfähiger VHD, können Sie einfach die WIM-Datei in die VHD kopieren. Ist es ein virtueller Computer, können Sie ihn direkt von der ISO-Datei starten.

Der Referenzcomputer startet Windows PE vom startfähigen LTI-Medium, anschließend startet sofort der Windows-Bereitstellungsassistent. Folgen Sie den Schritten in diesem Assistenten, wobei Sie unter anderem Ihre Anmeldeinformationen eingeben, auswählen, ob der Computer Mitglied einer Arbeitsgruppe oder Domäne ist, und so weiter. Sobald der Assistent abgeschlossen ist, wird das Betriebssystem Windows 7, inklusive aller Erweiterungen und Updates, die Sie zum ursprünglichen Installationsabbild hinzugefügt haben, auf dem Referenzcomputer installiert.

Sie müssen den Referenzcomputer gründlich testen. Sind Sie sicher, dass die Installation einwandfrei funktioniert, können Sie ein Abbild aufzeichnen, wie in Kapitel 2 beschrieben, und es mithilfe von MDT oder WDS bereitstellen.

Sollten Ihre Zielcomputer nicht PXE-kompatibel sein, müssen Sie sie vom startfähigen LTI-Medium starten. Microsoft empfiehlt, dass Sie bei PXE-Clientcomputern nicht diese Möglichkeit wählen, sondern stattdessen WDS und MDT 2010 nutzen, um solche Computer mit LTI bereitzustellen. WDS muss vorhanden sein, damit MDT 2010 LTI implementiert, das gilt aber nur, wenn Sie die Bereitstellung auf PXE-kompatiblen Computern durchführen.

Bereitstellen von Abbildern mit WDS

Kapitel 2 hat die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS) und WDS-Abbilder beschrieben. WDS wird als Serverrolle installiert, um Abbilder auf mehreren Computern bereitzustellen. Wenn Sie WDS einsetzen, hat das unter anderem den Vorteil, dass es mit Multicastübertragungen arbeitet. Daher braucht ein Betriebssystemabbild nur ein einziges Mal über das Netzwerk gesendet zu werden, auch wenn es auf mehreren Computern bereitgestellt wird.



Prüfungstipp

WDS ist zwar eine Serverrolle, aber das Thema wird in den Prüfungszielen für die Prüfung 70-680 mehrfach genannt. Daher können Sie damit rechnen, dass Fragen zu diesem Thema vorkommen.

Installieren und Konfigurieren von WDS

Sie installieren WDS als Serverrolle auf einem Server, der unter Windows Server 2008 oder Windows Server 2008 R2 läuft und Mitglied einer AD DS-Domäne (Active Directory Domain Services) ist. Weil WDS Bereitstellungen auf Clients durchführt, die PXE-kompatibel sind, brauchen Sie einen DHCP-Server (Dynamic Host Configuration Protocol) in Ihrem Netzwerk. Außerdem muss ein DNS-Server (Domain Name System) vorhanden sein, und Ihr

WDS-Bereitstellungsserver braucht ein NTFS-Volume für seinen Abbildspeicher. Sie müssen Mitglied der lokalen Gruppe *Administratoren* auf dem Server sein. Damit Sie über WDS Abbilder bereitstellen können, müssen Sie die Option *Bereitstellungsserver* auswählen, während Sie die Serverrolle installieren.

Sobald Sie die Serverrolle installiert haben, konfigurieren Sie den Server und fügen ein Startabbild sowie ein Installationsabbild hinzu. Der Server ist nun bereit, um Abbilder auf Zielcomputern bereitzustellen.

Beim Konfigurieren der WDS-Serverrolle gehen Sie folgendermaßen vor:

1. Öffnen Sie im Menü *Verwaltung* die Konsole *Windows-Bereitstellungsdienste*. Sofern noch kein Server im Knoten *Server* aufgelistet ist, müssen Sie mit der rechten Maustaste auf den Knoten klicken und *Server hinzufügen* wählen, um den lokalen Server hinzuzufügen.
2. Erweitern Sie im linken Fensterabschnitt der Konsole *Windows-Bereitstellungsdienste* den Knoten *Server*.
3. Klicken Sie mit der rechten Maustaste auf den lokalen Server und wählen Sie den Befehl *Server konfigurieren*.
4. Folgen Sie den Anweisungen im Assistenten.
5. Deaktivieren Sie nach Abschluss der Konfiguration das Kontrollkästchen *Abbilder jetzt dem Windows Deployment Server hinzufügen* und klicken Sie auf *Fertig stellen*.
6. Sie können die Einstellungen des Servers jederzeit ändern, indem Sie in der Konsole mit der rechten Maustaste auf den Server klicken und den Befehl *Eigenschaften* wählen.

Hinzufügen von Start- und Installationsabbildern

Wenn Sie den Server konfiguriert haben, fügen Sie Abbilder hinzu. Diese Abbilder umfassen ein *Startabbild* (die startfähige Umgebung, unter der Sie einen Zielcomputer anfangs starten) und mindestens ein *Installationsabbild* (die Abbilder, die Sie bereitstellen). Zuerst fügen Sie das Standardstartabbild (*Boot.wim*) hinzu, das auf dem Windows-Server oder der Windows 7-Installations-DVD enthalten ist. Die Datei *Boot.wim* enthält Windows PE und den WDS-Client. Sie gehen folgendermaßen vor, um das Standardstartabbild hinzuzufügen:

1. Klicken Sie im linken Fensterabschnitt der Konsole *Windows-Bereitstellungsdienste* mit der rechten Maustaste auf den Knoten *Startabbilder* und wählen Sie den Befehl *Startabbild hinzufügen*.
2. Wählen Sie das Standardstartabbild (*Boot.wim*) aus dem Ordner *\Sources* auf der Installations-DVD des Windows-Servers aus.
3. Klicken Sie auf *Öffnen* und dann auf *Weiter*.
4. Folgen Sie den Anweisungen im Assistenten, um das Abbild hinzuzufügen.

Installationsabbilder sind Betriebssystemabbilder, die Sie auf den Clientcomputern bereitstellen. Bei Windows 7 können Sie die Datei *Install.wim* von der Windows 7-Installations-DVD verwenden oder mit einem Windows 7-Referenzcomputer eigene Installationsabbilder erstellen. WDS kann ein Aufzeichnungsabbild verwenden, um das Abbild eines Referenzcomputers zu erstellen. Sie gehen folgendermaßen vor, um das Standardinstallationsabbild von einer Windows 7-Installations-DVD (*Install.wim*) hinzuzufügen:

1. Klicken Sie in der Konsole *Windows-Bereitstellungsdienste* mit der rechten Maustaste auf den Knoten *Installationsabbilder* und wählen Sie den Befehl *Installationsabbild hinzufügen*.
2. Geben Sie den Namen einer Abbildgruppe ein und klicken Sie auf *Weiter*.
3. Wählen Sie das Standardinstallationsabbild (*Install.wim*) aus dem Ordner *\Sources* auf der Windows 7-DVD aus und klicken Sie auf *Öffnen*.
4. Wenn Sie nicht alle Abbilder, die in der Datei *Install.wim* der DVD enthalten sind, hinzufügen wollen, können Sie die Kontrollkästchen der Abbilder deaktivieren, die Sie nicht brauchen. Fügen Sie nur Abbilder hinzu, für die Sie entsprechende Lizenzen besitzen.
5. Folgen Sie den Anweisungen im Assistenten.

Bereitstellen eines Installationsabbilds

Nun können Sie das Installationsabbild direkt auf PXE-kompatiblen Zielcomputern bereitstellen. In der Praxis werden Sie wohl kaum das Abbild, das Sie von der DVD kopiert haben, direkt auf mehreren Zielcomputern installieren, denn in diesem Fall wären die Computer durch bekannte Sicherheitsbedrohungen verwundbar.

Sie können das Abbild mit Sicherheitspatches, Treibern, Language Packs und anderen Paketen aktualisieren. Dafür stehen Tools wie DISM zur Verfügung. Oder Sie verwenden WDS mit MDT 2010, die in der Lage sind, Sicherheitspatches, Language Packs und Anwendungen hinzuzufügen. Selbst dann sollten Sie die Bereitstellung erst einmal auf einem einzelnen Referenzcomputer durchführen und ihn gründlich testen, bevor Sie das Abbild im gesamten Unternehmen bereitstellen. Haben Sie irgendwelche Änderungen an Ihrem Referenzcomputer vorgenommen, können Sie ein Aufzeichnungsabbild verwenden, um die neusten Einstellungen des Referenzcomputers aufzuzeichnen.

Sie gehen folgendermaßen vor, um ein Installationsabbild auf einem PXE-kompatiblen Zielcomputer bereitzustellen:

1. Konfigurieren Sie das BIOS des Zielcomputers so, dass der PXE-Start aktiviert ist, und stellen Sie die Startreihenfolge so ein, dass der Computer zuerst aus dem Netzwerk startet.
2. Starten Sie den Computer neu und drücken Sie F12, wenn Sie dazu aufgefordert werden, um den Netzwerkstart einzuleiten.
3. Falls mehrere Startabbilder auf dem WDS-Server zur Verfügung stehen, bekommen Sie auf dem Client ein Systemstartmenü angezeigt. Wählen Sie das gewünschte Startabbild aus.
4. Folgen Sie den Anweisungen in der Benutzeroberfläche der Windows-Bereitstellungsdienste.

Sobald die Installation abgeschlossen ist, wird der Zielcomputer neu gestartet und das Setup fortgesetzt.

Erstellen eines Suchabbilds

Wenn Sie Windows 7 auf einem Computer bereitstellen müssen, der nicht PXE-kompatibel ist, sollten Sie ein Suchabbild erstellen und es auf einem startfähigen Medium wie einer DVD oder einem startfähigen USB-Flashlaufwerk speichern. Wird der Zielcomputer mit diesem Suchabbild gestartet, ist er in der Lage, einen WDS-Server zu finden, der dann das

Installationsabbild auf dem Computer bereitstellt. Sie können Suchabbilder so konfigurieren, dass sie mit einem bestimmten WDS-Server kommunizieren. Wenn Sie mehrere WDS-Server in Ihrer Umgebung betreiben, können Sie für jeden ein eigenes Suchabbild erstellen.

Als Basis für das Suchabbild können Sie die Datei *Boot.wim* von der Windows Server 2008- oder Windows 7-Installations-DVD verwenden. Die Windows PE-Datei (*WinPE.wim*) aus dem Windows AIK eignet sich nicht, um ein Suchabbild zu erstellen. Beachten Sie aber, dass das Windows AIK auf dem WDS-Server installiert sein muss, um das startfähige Medium zu erstellen, auf dem das Suchabbild gespeichert wird. Sie gehen folgendermaßen vor, um ein Suchabbild zu erstellen und es auf einem startfähigen Medium zu installieren:

1. Erweitern Sie in der Konsole *Windows-Bereitstellungsdienste* den Knoten *Startabbilder*.
2. Klicken Sie mit der rechten Maustaste auf das Abbild, das Sie als Suchabbild verwenden wollen. Dies muss die Datei *Boot.wim* von der Windows-Server- oder Windows 7-DVD sein.
3. Wählen Sie den Befehl *Suchabbild erstellen*.
4. Folgen Sie den Anweisungen im Assistenten. Klicken Sie auf *Fertig stellen*, wenn die Erstellung abgeschlossen ist.
5. Um das Medium erstellen zu können, auf dem das Suchabbild gespeichert wird, müssen Sie das Windows AIK von *http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34* herunterladen und installieren.
6. Klicken Sie im Startmenü auf *Alle Programme* und dann auf *Eingabeaufforderung für Bereitstellungstools*.
7. Geben Sie den folgenden Befehl ein, um eine Windows PE-Buildumgebung zu generieren:

   ```
   copype <Architektur> c:\winpe
   ```

8. Führen Sie den folgenden Befehl aus, um das erstellte Suchabbild zu kopieren:

   ```
   copy /y c:\imagename.wim c:\winpe\iso\sources
   ```

9. Geben Sie den folgenden Befehl ein, um zurück in den Ordner *PETools* zu wechseln:

   ```
   cd c:\program files\windows aik\tools\petools
   ```

10. Geben Sie den folgenden Befehl ein, um das startfähige *.iso*-Abbild zu erstellen:

    ```
    oscdimg -n -bc:\winpe\iso\boot\etfsboot.com c:\winpe\iso c:\imagename.iso
    ```

11. Erstellen Sie eine startfähige DVD oder ein USB-Flashlaufwerk aus dem ISO-Abbild. Wenn Sie das Abbild auf einen Windows 7-Client (oder Windows Vista-Client) übertragen, brauchen Sie dafür nur doppelt auf das Abbild zu klicken. Sie können aber auch ein allgemein anerkanntes Produkt eines anderen Softwareherstellers verwenden.

Erstellen eines Aufzeichnungsabbilds

Aufzeichnungsabbilder sind Startabbilder, die Sie auf einem Clientcomputer starten, um sein Betriebssystem in einer WIM-Datei aufzuzeichnen. Sie erstellen ein Aufzeichnungsabbild, indem Sie auf dem Referenzcomputer Sysprep ausführen, ihn neu starten, die Taste F12 drücken (oder ein Suchabbild verwenden, falls der Referenzcomputer nicht PXE-kompatibel ist), das Aufzeichnungsabbild auswählen, das nun im Systemstartmenü aufgelistet werden

müsste, das Abbild des Referenzcomputers als WIM-Abbild aufzeichnen und es auf den WDS-Server hochladen.

Beachten Sie, dass Sie auch das Tool ImageX aus dem Windows AIK verwenden können, um ein Systemabbild aufzuzeichnen und auf dem WDS-Server zu installieren. Ein Aufzeichnungsabbild automatisiert diesen Prozess aber. Normalerweise erstellen Sie ein Aufzeichnungsabbild aus der Datei *Boot.wim*. Dabei gehen Sie folgendermaßen vor:

1. Erweitern Sie in der Konsole *Windows-Bereitstellungsdienste* den Knoten *Startabbilder*.
2. Klicken Sie mit der rechten Maustaste auf das Abbild, das Sie als Aufzeichnungsabbild verwenden wollen (normalerweise *Boot.wim*).
3. Wählen Sie den Befehl *Aufzeichnungsstartabbild erstellen*.
4. Geben Sie einen Namen, eine Beschreibung und den Speicherort an, an dem Sie eine lokale Kopie der Datei speichern wollen. Diesen Ordner geben Sie für den Fall an, dass ein Netzwerkproblem auftritt, während Sie das Aufzeichnungsabbild bereitstellen.
5. Folgen Sie den Anweisungen des Assistenten. Klicken Sie auf *Fertig stellen*, wenn das Abbild fertig ist.
6. Klicken Sie mit der rechten Maustaste auf den Ordner *Startabbilder*.
7. Wählen Sie den Befehl *Startabbild hinzufügen*.
8. Wählen Sie das neue Aufzeichnungsabbild aus und klicken Sie auf *Weiter*.
9. Folgen Sie den Anweisungen des Assistenten.

WDS-Abbilder

In den letzten Abschnitten haben Sie erfahren, wie WDS Installations-, Start-, Aufzeichnungs- und Suchabbilder erstellt. An dieser Stelle ist es daher sinnvoll, noch einmal den Einsatzzweck dieser unterschiedlichen Abbilder zusammenzufassen. WDS installiert ein Installationsabbild (üblicherweise eine WIM-Datei) auf den Zielcomputern. Im Unterschied zu MDT 2010 kann WDS diese Datei nicht verändern, indem es Treiber, Language Packs und Anwendungen zur Bereitstellungsfreigabe hinzufügt. Aber Sie können das WIM-Abbild mit DISM bearbeiten, bevor Sie es mit WDS verteilen. Sie können das WDS-Abbild außerdem auf einem Referenzcomputer bereitstellen, es testen und bei Bedarf online aktualisieren, um sicherzustellen, dass es auf dem neusten Stand ist. Dann verallgemeinern Sie es mit Sysprep und erstellen mithilfe des Aufzeichnungsabbilds ein neues Installationsabbild auf dem WDS-Server.

WDS startet die Zielcomputer zuerst mit einem Startabbild. So kann die Bereitstellung des Installationsabbilds auf den Zielcomputern durchgeführt werden.

WDS ist auch in der Lage, ein Abbild auf einem Referenzcomputer aufzuzeichnen und es auf mehreren Zielcomputern zu installieren. Dazu wird der Referenzcomputer von einem speziellen Typ Startabbild gestartet, dem sogenannten Aufzeichnungsabbild. Ein Aufzeichnungsabbild enthält Windows PE und den Assistenten zur Abbildaufzeichnung der Windows-Bereitstellungsdienste. Sobald der Referenzcomputer mit einem Aufzeichnungsabbild gestartet wurde (nachdem Sie ihn mit Sysprep vorbereitet haben), erstellt der Assistent ein Installationsabbild des Computers und speichert es als WIM-Datei. Dies wird dann das Installationsabbild, das WDS auf den Zielcomputern bereitstellt, nachdem diese unter einem Standardstartabbild gestartet wurden.

Normalerweise arbeitet WDS mit PXE-fähigen Computern. Mithilfe von PXE können Computer über das Netzwerk starten und dem Benutzer ein Menü anbieten, in dem er ein WDS-Startabbild auswählt. Aber auch wenn die Zielcomputer nicht PXE-kompatibel sind, kann WDS ein Betriebssystem darauf bereitstellen. Dazu werden die Computer zuerst von einem Suchabbild gestartet. Wenn Sie einen Computer unter einem Suchabbild starten, sucht der WDS-Client einen gültigen WDS-Server, woraufhin Sie wiederum das Abbild auswählen, das Sie bereitstellen wollen.



Hinweis WDS und Windows PE-Standardabbilder

Das WDS-Suchabbild enthält ein Windows PE-Abbild und die WDS-Clientsoftware. Sie sollten Windows PE nicht von einem Windows PE-Startdatenträger starten, wenn Sie versuchen, auf einen WDS-Server zuzugreifen. Sie sollten einen Zielcomputer auch nicht unter Windows PE oder von einem Suchabbild starten, wenn er PXE-kompatibel ist.

Einen Zielcomputer manuell starten

Wenn ein Computer nicht PXE-kompatibel ist und Sie ihn von Hand mit einem Suchabbild starten müssen, können Sie optische Medien oder andere Wechseldatenträger verwenden, beispielsweise eine USB-Festplatte oder einen USB-Flashstick. Startfähige Medien können Sie unter anderem mit den Tools BCDEdit und BCDBoot erstellen. In Kapitel 2 wurde das Tool BCDEdit beschrieben; dort wird erklärt, wie Sie eine VHD als startfähig markieren. Dieselbe Technik können Sie auch für USB-Geräte nutzen.

BCDboot ist ein Windows AIK-Tool, mit dem Sie eine Systempartition einrichten oder die Startumgebung reparieren, die in der Systempartition liegt. Das Tool legt eine Systempartition an, indem es einen kleinen Teil der Startumgebungsdateien aus einem installierten Windows-Abbild kopiert. Mit BCDboot können Sie auch einen neuen Starteintrag im BCD-Speicher der Systempartition anlegen, über den Sie das installierte Windows-Abbild starten. Sie können BCDboot aus Windows PE heraus ausführen. Auch wenn Sie das Windows AIK nicht installiert haben, steht BCDboot im Verzeichnis *Windows\System32* zur Verfügung. Das Tool ist außerdem im Windows OEM Preinstallation Kit (OPK) enthalten.

Bestimmte BCD-Einstellungen können in der BCD-Vorlagendatei definiert werden. Das Tool kopiert die neusten Versionen der Startumgebungsdateien aus den Ordnern *Windows\Boot* und *Windows\System32* des Betriebssystemabbilds in die Standardsystempartition, die von der Firmware identifiziert wird. Diese Partition können Sie mithilfe eines Partitionierungstools wie DiskPart anlegen.

Nachdem ein Computer unter Windows PE gestartet wurde und ein Abbild installiert ist, initialisieren Sie mithilfe von BCDBoot den BCD-Speicher und kopieren die Startumgebungsdateien in die Systempartition. So ist der Computer in der Lage, normal zu starten, wenn er ohne Windows PE neu gestartet wird.



Weitere Informationen Diskpart

Weitere Informationen über Diskpart finden Sie unter *http://support.microsoft.com/kb/300415*. Dieser Artikel wurde zwar für Windows XP geschrieben, er wurde seitdem aber aktualisiert, sodass die Informationen auch für Windows 7 gelten. Das Tool Diskpart wird in Kapitel 4, »Verwalten von Geräten und Datenträgern«, ausführlich beschrieben.



Weitere Informationen BCDBoot

Weitere Informationen über BCDBoot finden Sie unter *http://technet.microsoft.com/en-us/library/dd744347%28WS.10%29.aspx*.

Arbeiten mit dem Tool WDSUTIL

WDS stellt ein GUI-Tool und ein Befehlszeilentool zur Verfügung. Die meisten Bereitstellungsaufgaben können Sie in der Konsole *Windows-Bereitstellungsdienste* erledigen. Hier können Sie beispielsweise die Richtlinie zum automatischen Hinzufügen konfigurieren und ausstehende Computer genehmigen oder abweisen. Wollen Sie Clientcomputer allerdings vorab bereitstellen, müssen Sie das Befehlszeilentool WDSUTIL verwenden.

Zum Beispiel können Sie mit dem WDSUTIL-Argument `/add` Abbilder und Abbildgruppen hinzufügen oder Computer vorab bereitstellen. Der folgende Befehl stellt den Computer *Aberdeen* mit der MAC-Adresse 00-13-E8-64-46-01 vorab bereit:

```
WDSUTIL /Add-Device /Device:Aberdeen /ID: 00-13-E8-64-46-01
```

Der nächste Befehl fügt ein Startabbild zum WDS-Server hinzu. Das Abbild heißt *Myboot.wim*, es ist in *C:\MybootImages* gespeichert:

```
WDSUTIL /Add-Image /ImageFile:"C:\mybootimages\myboot.wim" /ImageType:Boot
```

Mit dem Tool WDSUTIL können Sie folgende Aufgaben erledigen:

- Konfigurieren eines WDS-Servers für den ersten Einsatz
- Starten und Beenden aller Dienste auf dem WDS-Server
- Aktualisieren von Dateien in der Freigabe *RemoteInstall*
- Zurücknehmen der Änderungen, die während der Serverinitialisierung vorgenommen wurden
- Erstellen neuer Aufzeichnungs- und Suchabbilder sowie Implementieren von Multicastübertragungen und Namespaces
- Hinzufügen von Abbildern und Abbildgruppen sowie Vorabbereitstellen von Computern
- Genehmigen oder Abweisen von Computern, für die die Genehmigung eines Administrators aussteht
- Kopieren eines Abbilds innerhalb des Abbildspeichers
- Exportieren eines Abbilds aus dem Abbildspeicher in eine *.wim*-Datei
- Ersetzen eines Start- oder Installationsabbilds durch eine neue Version
- Entfernen von Abbildern, Abbildgruppen, Multicastübertragungen und Namespaces
- Konvertieren eines vorhandenen RIPrep-Abbilds (Remote Installation Preparation) in eine Windows-Abbilddatei (*.wim*)
- Löschen von Computern, die in der Datenbank der Geräte eingetragen sind, die automatisch hinzugefügt werden. Diese Datenbank speichert Informationen über die Computer auf dem Server.
- Deaktivieren oder Aktivieren aller Dienste für WDS
- Trennen der Verbindung zu einem Client bei einer Multicastübertragung

- Ändern von Eigenschaften und Attributen eines angegebenen Objekts
- Abrufen von Eigenschaften und Attributen eines angegebenen Objekts
- Anzeigen des Fortschritts, während ein Befehl ausgeführt wird



Weitere Informationen WDSUTIL

Weitere Informationen über WDSUTIL, darunter die Syntax und Codebeispiele, finden Sie unter *http://technet.microsoft.com/en-us/library/cc771206.aspx*.



Weitere Informationen WDS

Weitere Informationen über WDS erhalten Sie, wenn Sie unter *http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3cb929bc-af77-48d2-9b51-48268cd235fe* die WDS-Dokumentation (in englischer Sprache) herunterladen. Unter *http://technet.microsoft.com/de-de/library/cc771670%28WS.10%29.aspx* können Sie eine deutsche Version der Schritt-für-Schritt-Anleitung online lesen.

Verwenden von SCCM 2007

SCCM 2007 (ConfigMgr) ist Software für Windows Server 2003 oder Windows Server 2008, die eine Änderungs- und Konfigurationsverwaltung für Microsoft-Plattformen implementiert. Unter anderem können Sie damit folgende Aufgaben erledigen:

- Bereitstellen von Betriebssystemen, Softwareanwendungen und Softwareupdates
- Messen der Softwarenutzung
- Erkennen von Abweichungen gegenüber der gewünschten Konfiguration
- Inventarisieren von Hardware und Software
- Administrieren von Computern über das Netzwerk

SCCM 2007 sammelt Informationen in einer SQL Server-Datenbank, die Sie konfigurieren können. Dafür greift es auf Tools wie MDT 2010 zurück. Auf diese Weise ist es möglich, Abfragen und Berichte zu erstellen, die Informationen aus der gesamten Organisation zusammenführen. SCCM 2007 kann eine große Bandbreite von Microsoft-Betriebssystemen verwalten, darunter Clientplattformen, Serverplattformen und mobile Geräte. Es arbeitet mit MDT 2010 zusammen, um ZTI zu implementieren.

SCCM 2007 stellt ein Hardware- und Softwareinventar zusammen und verteilt und installiert Softwareanwendungen und Softwareupdates wie beispielsweise Sicherheitsfixes. Es arbeitet mit Windows Server 2008-Netzwerkrichtlinienservern (Network Policy Server, NPS) zusammen, um zu verhindern, dass Computer, die bestimmte Anforderungen nicht erfüllen (weil beispielsweise bestimmte Sicherheitsupdates nicht installiert sind), auf das Netzwerk zugreifen. SCCM 2007 legt fest, wie die erwünschte Konfiguration für einen oder mehrere Computer aussieht, und überwacht, ob diese Konfiguration eingehalten wird. Es steuert Computer im Remotezugriff, um Support im Rahmen einer Problembehandlung zu gewährleisten.

Schnelltest

- Mit welchem Befehlszeilenprogramm können Sie Zielcomputer bei der Systemabbildbereitstellung vorab bereitstellen?

Antwort zum Schnelltest

- WDSUTIL

SCCM-Clients und -Standorte

Sobald Sie Ihren zentralen SCCM 2007-Standort installiert haben, können Sie Clients und Ressourcen zu diesem Standort hinzufügen. Dafür nutzen Sie eine der verfügbaren SCCM-Suchmethoden, die Ihr Netzwerk nach Ressourcen durchsuchen, die Sie mit SCCM verwenden können. Sie müssen die Computer in Ihrem Netzwerk auf diese Weise finden, bevor Sie die Configuration Manager-Clientsoftware installieren können, die es ermöglicht, Elemente wie Pakete und Updates an die Clients zu verteilen. Es stehen folgenden Suchmethoden zur Verfügung:

- Takterkennung
- Netzwerkerkennung
- Active Directory-Benutzer
- Active Directory-Systemgruppen
- Active Directory-Sicherheitsgruppen
- Active Directory-Systemerkennung



Weitere Informationen Clientsuche in SCCM

Eine ausführliche Beschreibung der Clientsuche würde den Rahmen der Prüfung 70-680 und dieses Buchs sprengen. Bei Interesse können Sie sich unter *http://msdn.microsoft.com/en-us/library/cc143989.aspx* zu diesem Thema informieren.

Hat SCCM 2007 Clients gefunden, installiert es Clientsoftware auf allen Windows-Computern, die es verwaltet. Configuration Manager 2007-Clientsoftware kann auf Desktopcomputern, Servern, tragbaren Computern wie Notebooks, mobilen Geräten mit Windows Mobile oder Windows CE und Geräten mit Windows XP Embedded (beispielsweise Geldautomaten) installiert werden.

Sie können in SCCM 2007 Clients in Standorten zusammenfassen. SCCM-Standorte fassen Clients zu einfach verwaltbaren Gruppen zusammen, die ähnliche Anforderungen bezüglich Features, Bandbreite, Konnektivität, Sprache und Sicherheit aufweisen. SCCM 2007-Standorte können mit Ihren AD DS-Standorten übereinstimmen oder völlig unabhängig davon sein. Clients können zwischen Standorten verschoben oder von Remotestandorten wie privaten Arbeitszimmern verwaltet werden.

Clients kommunizieren mit Standortsystemen, die Standortsystemrollen hosten. Standortsysteme kommunizieren mit dem Standortserver und der Standortdatenbank. Sind mehrere Standorte innerhalb einer Hierarchie verbunden, kommunizieren sie mit ihren direkten übergeordneten, direkten untergeordneten und manchmal auch über mehrere Ebenen untergeordneten Standorten. SCCM 2007 nutzt Grenzen, um festzustellen, ob sich Clients und Standort-

systeme innerhalb oder außerhalb des Standorts befinden. Grenzen können IP-Subnetze, IP-Adressbereiche, IPv6-Präfixe und AD DS-Standorte sein. Zwei Standorte sollten niemals dieselben Grenzen definieren.

Wenn SCCM 2007-Features innerhalb desselben Standorts miteinander kommunizieren, verwenden sie entweder SMB (Server Message Block), HTTP (Hypertext Transfer Protocol) oder HTTPS (Hypertext Transfer Protocol Secure); das verwendete Protokoll hängt von verschiedenen Standortkonfigurationseinstellungen ab, die Sie vornehmen. Weil diese gesamte Kommunikation unverwaltet abläuft, sollten Sie sicherstellen, dass diese Standortelemente schnelle Kommunikationskanäle besitzen.

Der Tasksequenz-Editor von SCCM 2007

SCCM 2007 verwendet Tasksequenzen, ganz ähnlich wie MDT 2010. Sie können Tasksequenzen zwischen diesen Tools austauschen. Der Tasksequenz-Editor von SCCM 2007 erstellt und bearbeitet Tasksequenzen, die in Gruppen von Tasksequenzschritten organisiert sind. Je nachdem, ob Sie im Tasksequenzerstellungs-Assistenten *Bestehendes Abbildpaket installieren* oder *Referenz-Betriebssystemabbild erstellen* ausgewählt haben, enthält die Tasksequenz eine Reihe grundlegender Tasksequenzgruppen und -schritte. Wenn Sie im Tasksequenzerstellungs-Assistenten dagegen *Neue benutzerdefinierte Tasksequenz erstellen* auswählen, wird eine leere Tasksequenz erstellt.

Der Tasksequenz-Editor zeigt die Tasksequenzgruppen und -schritte in der Strukturansicht an der linken Seite des Editorfensters an, ähnlich wie der Tasksequenz-Editor von MDT 2010. Wenn Sie eine Tasksequenzgruppe oder einen Tasksequenzschritt auswählen, werden die Eigenschaften neben der Strukturansicht in Registerkarten angezeigt, die Sie auswählen, um verschiedene Einstellungen zu konfigurieren. Tasksequenzgruppen und -schritte können innerhalb anderer Tasksequenzgruppen verschachtelt werden.

Tasksequenzschritte sind in den Gruppen *Allgemein*, *Datenträger*, *Benutzerstatus*, *Abbilder*, *Treiber* und *Einstellungen* zusammengefasst. Allgemeine SCCM-Tasksequenzschritte sind:

- **Befehlszeile ausführen** Dieser Tasksequenzschritt führt beliebige Befehlszeilen aus. Die Tasksequenzaktion kann in einem Standardbetriebssystem oder Windows PE ausgeführt werden.
- **Software installieren** Dieser Tasksequenzschritt gibt ein SCCM 2007-Paket und -Programm an, die im Rahmen der Tasksequenz installiert werden. Die Installation beginnt sofort, es wird nicht auf ein konfiguriertes Abrufintervall gewartet. Der Tasksequenzschritt *Software installieren* läuft nur in einem Standardbetriebssystem wie Windows 7, aber nicht unter Windows PE.
- **Softwareupdates installieren** Dieser Tasksequenzschritt installiert Softwareupdates auf einem Zielcomputer. Wird dieser Tasksequenzschritt ausgeführt, wird untersucht, ob Softwareupdates auf den Zielcomputer angewendet werden müssen. Der Schritt installiert insbesondere Softwareupdates, die für Sammlungen konfiguriert wurden, deren Mitglied der Computer ist. Der Tasksequenzschritt *Softwareupdates installieren* läuft nur in einem Standardbetriebssystem wie Windows 7, aber nicht unter Windows PE.
- **Einer Domäne oder Arbeitsgruppe beitreten** Diese Tasksequenzaktion fügt einen Zielcomputer zu einer Arbeitsgruppe oder Domäne hinzu. Der Tasksequenzschritt *Einer Domäne oder Arbeitsgruppe beitreten* läuft nur in einem Standardbetriebssystem wie Windows 7, aber nicht unter Windows PE.

- **Verbindung mit Netzwerkordner herstellen** Diese Tasksequenzaktion baut eine Verbindung zu einem freigegebenen Netzwerkordner auf. Der Tasksequenzschritt *Verbindung mit Netzwerkordner herstellen* läuft nur in einem Standardbetriebssystem wie Windows 7, aber nicht unter Windows PE.
- **Computer neu starten** Dieser Tasksequenzschritt startet den Computer neu, der die Tasksequenz ausführt. Nach dem Neustart macht der Computer automatisch mit dem nächsten Schritt der Tasksequenz weiter. Die Tasksequenzaktion *Computer neu starten* kann sowohl in einem Standardbetriebssystem als auch in Windows PE ausgeführt werden.
- **Tasksequenzvariable festlegen** Dieser Tasksequenzschritt ändert den Wert einer Tasksequenzvariablen, die für die Tasksequenz benutzt wird. Tasksequenzaktionen lesen Tasksequenzvariablen, die das Verhalten dieser Aktionen steuern.



Weitere Informationen Tasksequenzaktionen und -variablen

Weitere Informationen über Tasksequenzaktionen finden Sie unter *http://technet.microsoft.com/de-de/library/bb632625.aspx*, weitere Informationen über Tasksequenzvariablen unter *http://technet.microsoft.com/de-de/library/bb632442.aspx*.

Mit Schritten aus den Gruppen *Datenträger*, *Benutzerstatus*, *Abbilder*, *Treiber* und *Einstellungen* können Sie folgende Elemente von SCCM-Clients konfigurieren:

- Datenträger
  - Festplatte formatieren und partitionieren
  - In dynamischen Datenträger konvertieren
  - BitLocker aktivieren und deaktivieren
- Benutzerstatus
  - Statusspeicher anfordern
  - Statusspeicher freigeben
  - Benutzerstatus aufzeichnen
  - Benutzerstatus wiederherstellen
- Abbilder
  - Anwenden des Betriebssystems
  - Anwenden des Datenabbilds
  - Installieren von Bereitstellungstools
  - Vorbereiten des ConfigMgr-Clients für die Aufzeichnung
  - Vorbereiten von Windows für die Aufzeichnung
  - Aufzeichnen des Betriebssystemabbilds
- Treiber
  - Treiber automatisch anwenden
  - Treiberpaket anwenden
  - Schritte festlegen
  - Netzwerkeinstellungen aufzeichnen

- Windows-Einstellungen aufzeichnen
- Netzwerkeinstellungen anwenden
- Windows-Einstellungen anwenden

Integration von SCCM 2007 und MDT 2010

SCCM 2007 und MDT 2010 können in der Configuration Manager-Konsole auf einem Distributionsserver integriert werden, um Aufgaben wie das Installieren von Language Packs zu ermöglichen. Meist werden die beiden Tools allerdings integriert, um ZTI zu implementieren. Sie müssen MDT 2010 auf jedem Computer installieren, der die Configuration Manager-Konsole ausführt. Anschließend können Sie die Integrationsoption von SCCM 2007 implementieren und Daten für MDT 2010-Pakete angeben.

Damit die SCCM-Integrationsfeatures von MDT 2010 zur Verfügung stehen, müssen Sie das Skript für die Integrationskonfiguration von Configuration Manager 2007 ausführen. Dieses Skript kopiert alle benötigten SCCM-Integrationdateien in *Configuration Manager 2007_root* (wobei *Configuration Manager 2007_root* der Ordner ist, in dem SCCM installiert wurde). Das Skript fügt außerdem WMI-Klassen (Windows Management Instrumentation) für die neuen benutzerdefinierten Aktionen von MDT 2010 hinzu. Dazu wird eine *.mof*-Datei (Managed Object Format) kompiliert, die die neuen Klassendefinitionen enthält. Die *.mof*-Datei bildet den Mechanismus, mit dem Informationen über WMI-Klassen in das WMI-Repository eingetragen werden.

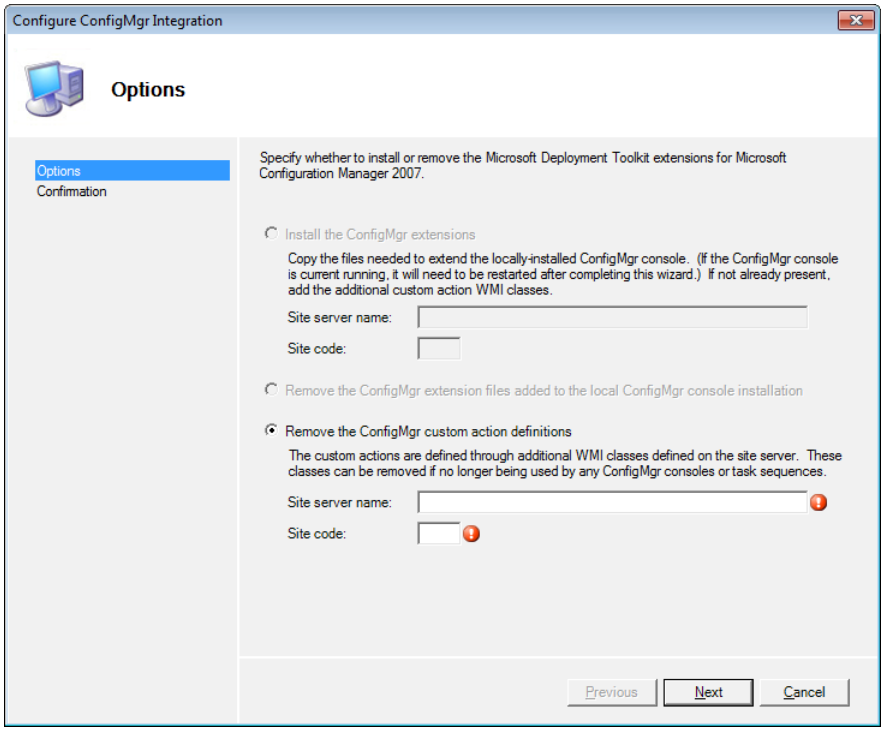

Configure ConfigMgr Integration
Options
Options
Confirmation
Specify whether to install or remove the Microsoft Deployment Toolkit extensions for Microsoft Configuration Manager 2007.
Install the ConfigMgr extensions
Copy the files needed to extend the locally-installed ConfigMgr console. (If the ConfigMgr console is current running, it will need to be restarted after completing this wizard.) If not already present, add the additional custom action WMI classes.
Site server name:
Site code:
Remove the ConfigMgr extension files added to the local ConfigMgr console installation
Remove the ConfigMgr custom action definitions
The custom actions are defined through additional WMI classes defined on the site server. These classes can be removed if no longer being used by any ConfigMgr consoles or task sequences.
Site server name:
Site code:
Previous
Next
Cancel

Abbildung 3.32 Einstellen der Optionen für die Integration von SCCM 2007

Bevor Sie das Skript für die Integrationskonfiguration von Configuration Manager 2007 ausführen, müssen Sie die Configuration Manager-Konsole schließen. Sie gehen folgendermaßen vor, um dieses Skript auszuführen:

1. Klicken Sie im Menü *Alle Programme* auf *Microsoft Deployment Toolkit* und dann auf *Configure ConfigMgr Integration*. Abbildung 3.32 zeigt die Seite *Options* des Assistenten *Configure ConfigMgr Integration* (noch ohne eingetragene Werte).
2. Geben Sie im Textfeld *Site server name* den Namen des SCCM 2007-Servers ein, auf dem Sie die MDT 2010-Integration implementieren wollen.
3. Geben Sie im Textfeld *Site code* den SCCM-Standortcode ein, in dem die MDT 2010-Integration installiert wird, und klicken Sie auf *Next*.

Nun können Sie Ihre Bereitstellung mithilfe der Features und Tools verwalten, die von MDT 2010 in Kombination mit SCCM-Features wie Clienterkennung und Clientintegrationsmethoden zur Verfügung gestellt werden, um eine vollständig automatisierte Bereitstellung anzubieten, die ganz ohne Benutzereingaben auskommt.



Weitere Informationen SCCM 2007 und die Installation von Softwareupdates

Weitere Informationen, wie Sie SCCM 2007 und die vordefinierte Tasksequenz *Softwareupdates installieren* verwenden, finden Sie unter *http://technet.microsoft.com/de-de/library/bb632402.aspx*.

Ein Abbild von Hand installieren

Manchmal ist es schlicht nicht sinnvoll, ausgefeilte Bereitstellungstools wie MDT 2010, SCCM 2007 oder WDS einzusetzen. Nehmen wir an, Sie haben einen Windows 7-Computer in Ihrem SOHO-Netzwerk (Small Office/Home Office) installiert, die Installation mit Sysprep verallgemeinert und mit dem Skript *Copype.cmd* eine startfähige Windows PE-DVD (oder eine startfähige USB-Festplatte oder einen USB-Flashstick) erstellt.

Sie haben das Tool ImageX in das Unterverzeichnis *Iso* auf dem Windows PE-Medium kopiert, Ihren Computer unter Windows PE gestartet und mit ImageX ein WIM-Abbild der Computerinstallation angefertigt. Schließlich haben Sie die fertige WIM-Datei auf Ihr Windows PE-Medium kopiert (und unter Umständen mit DISM weitere Treiber hinzugefügt).

Nun wollen Sie dieses angepasste Abbild auf die Festplatten von zwei neuen Computern anwenden, die Sie ohne Betriebssystem gekauft haben. Sie starten jeden Computer vom Windows PE-Medium und installieren mit ImageX das Abbild. Im letzten Schritt machen Sie das Abbild startfähig, indem Sie von Windows PE aus mit BCDboot den BCD-Speicher initialisieren und die Startumgebungsdateien auf die Systempartition kopieren. Sobald Sie einen der Computer neu starten, läuft er unter Windows 7 und hat dieselben Einstellungen konfiguriert und Anwendungen installiert wie Ihr ursprünglicher Computer. Achten Sie darauf, dass Sie keine Lizenzbedingungen verletzen.

Übung Herunterladen, Installieren und Konfigurieren von MDT 2010

In dieser Übung laden Sie die Installations- und Dokumentationsdateien von MDT 2010 herunter und installieren das Toolkit. Mit der Deployment Workbench legen Sie eine Bereitstellungsfreigabe an und installieren ein Abbild.

Übung 1 Herunterladen der Installationsdateien und der Dokumentation zu MDT 2010

In dieser Übung laden Sie das MDT und die zugehörige Dokumentation von der Downloadseite *http://www.microsoft.com/downloads/details.aspx?FamilyId=3BD8561F-77AC-4400-A0C1-FE871C461A89&displaylang=en* herunter. Sie haben hier die Möglichkeit, folgende Dateien einzeln herunterzuladen:

- *MicrosoftDeploymentToolkit_x64.msi*
- *MicrosoftDeploymentToolkit_x86.msi*
- *New in MDT 2010.docx*
- *Release Notes.docx*
- *Optional – MDT 2010 Print-Ready Documentation.zip*

Sie sollten die passende Version für Ihr Betriebssystem herunterladen und installieren – dieses Buch beschreibt die 32-Bit-Version (x86). Sie brauchen keine zusätzliche Software, um MDT unter Windows 7 auszuführen. Wenn Sie allerdings MDT in Kombination mit SCCM 2007 auf einem Bereitstellungsserver verwenden, müssen Sie neben diesen Anwendungen noch zusätzliche Software wie SQL Server installieren.

Gehen Sie folgendermaßen vor, um MDT 2010 und die zugehörige Dokumentation herunterzuladen:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Legen Sie einen Ordner an, in dem Sie die heruntergeladenen Dateien speichern, beispielsweise *C:\Windows 7\MDT 2010 Files*. Erstellen Sie außerdem einen Ordner für die Dokumentation, zum Beispiel *C:\Windows 7\MDT 2010 Documentation*.
3. Öffnen Sie den Internet Explorer und rufen Sie die Seite *http://www.microsoft.com/downloads/details.aspx?FamilyId=3BD8561F-77AC-4400-A0C1-FE871C461A89&displaylang=en* auf.
4. Blättern Sie auf der Seite nach unten zu *Files in This Download* (Abbildung 3.33).

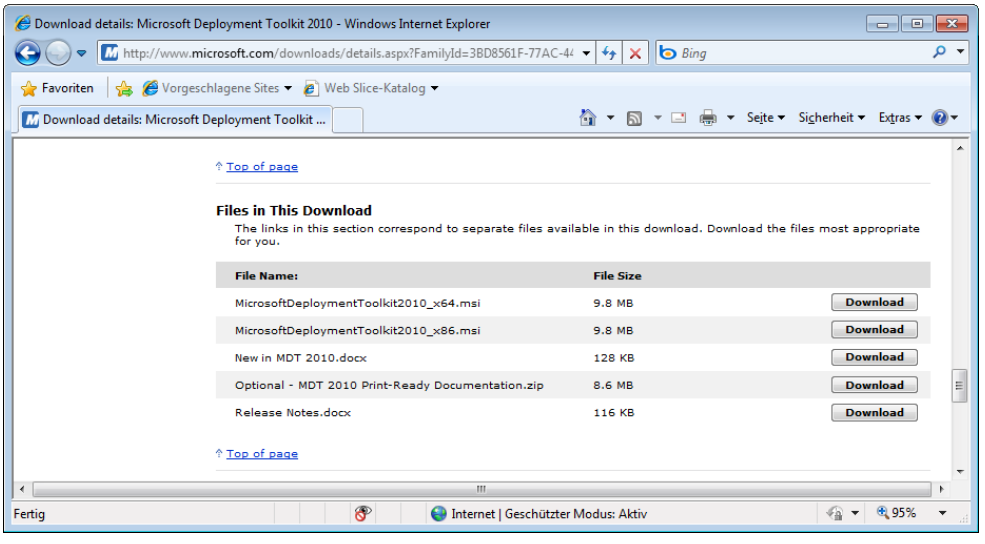

Download details: Microsoft Deployment Toolkit 2010 - Windows Internet Explorer
http://www.microsoft.com/downloads/details.aspx?FamilyId=3BD8561F-77AC-44
Bing
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Download details: Microsoft Deployment Toolkit ...
Seite
Sicherheit
Extras
Top of page
Files in This Download
The links in this section correspond to separate files available in this download. Download the files most appropriate for you.
File Name:
File Size
MicrosoftDeploymentToolkit2010_x64.msi 9.8 MB Download
MicrosoftDeploymentToolkit2010_x86.msi 9.8 MB Download
New in MDT 2010.docx 128 KB Download
Optional - MDT 2010 Print-Ready Documentation.zip 8.6 MB Download
Release Notes.docx 116 KB Download
Top of page
Fertig
Internet | Geschützter Modus: Aktiv
95%

Abbildung 3.33 Auswählen, welche Dateien heruntergeladen werden

5. Klicken Sie auf die Schaltfläche *Download* neben der Datei *MicrosoftDeployment-Toolkit2010_x86.msi*.
6. Geben Sie an, dass die Datei auf Festplatte gespeichert werden soll, und wählen Sie *C:\Windows 7\MDT 2010 Files* als Zielordner. Warten Sie, bis der Download abgeschlossen ist.
7. Laden Sie auf dieselbe Weise die Datei *MicrosoftDeploymentToolkit2010_x64.msi* herunter.
8. Prüfen Sie, ob die heruntergeladenen Dateien empfangen wurden und im Ordner *C:\Windows 7\MDT 2010 Files* liegen.
9. Laden Sie auf dieselbe Weise die drei Dokumentationsdateien herunter.
10. Prüfen Sie, ob die Dokumentationsdateien im Ordner *C:\Windows 7\MDT 2010 Documentation* liegen.

Übung 2 Lesen der MDT 2010-Dokumentation

Microsoft empfiehlt, die MDT 2010-Dokumentation zu lesen, bevor Sie das Tool installieren. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Öffnen Sie den Ordner *C:\Windows 7\MDT 2010 Documentation* und klicken Sie doppelt auf *Optional – MDT 2010 Print-Ready Documentation.zip*, um die ZIP-Datei zu öffnen (Abbildung 3.34).

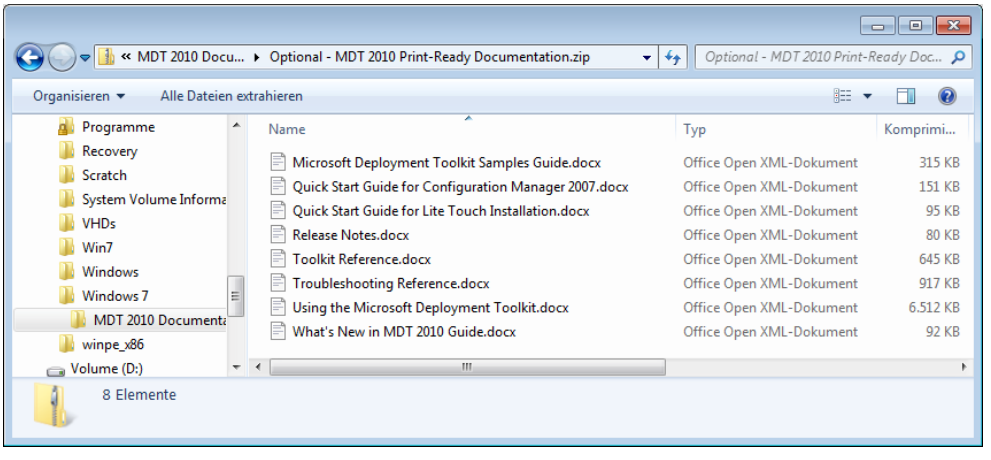


Abbildung 3.34 Die Dokumentationsdateien zu MDT 2010

3. Klicken Sie auf *Quick Start Guide for Lite Touch Installation.docx* und speichern Sie die Datei in *C:\Windows 7\MDT 2010 Documentation*.
4. Wechseln Sie wieder in den Ordner *C:\Windows 7\MDT 2010 Documentation*. Klicken Sie doppelt auf *Release Notes.docx* und speichern Sie die Datei im selben Ordner.
5. Lesen Sie die Dokumente *Release Notes.docx*, *What's New In MDT 2010 Guide.docx* und *Quick Start Guide for Lite Touch Installation.docx* sorgfältig durch, bevor Sie Übung 3 in Angriff nehmen.

Übung 3 Installieren von MDT 2010

In dieser Übung installieren Sie MDT 2010. Dabei wird vorausgesetzt, dass Sie die x86-Version von Windows 7 Ultimate installiert haben. Falls Sie ein 64-Bit-Betriebssystem verwenden, müssen Sie stattdessen die x64-Version von MDT 2010 installieren. Gehen Sie folgendermaßen vor, um MDT 2010 zu installieren:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Klicken Sie mit der rechten Maustaste auf die Datei *MicrosoftDeploymentToolkit_x86.msi*, die Sie in Übung 1 heruntergeladen haben, und wählen Sie den Befehl *Installieren*.
3. Klicken Sie auf der Seite *Welcome* auf *Next*.
4. Lesen Sie sich auf der Seite *End-User License Agreement* die Lizenzvereinbarung durch. Wählen Sie die Option *I accept the terms in the License Agreement* aus und klicken Sie auf *Next*, wenn Sie mit den Vereinbarungen einverstanden sind.
5. Wählen Sie auf der Seite *Custom Setup* (Abbildung 3.35) die Features, die installiert werden sollen, und den Zielordner für die Installation aus und klicken Sie auf *Next*. Es stehen folgende Features zur Verfügung:
   - **Documents** Dieses Feature installiert den Leitfaden und das Hilfsmaterial. In der Standardeinstellung werden die Dokumente im Ordner *C:\Program Files\Microsoft Deployment Toolkit\Documentation* gespeichert. Um dieses Feature installieren und die Dokumente mit der Deployment Workbench ansehen zu können, müssen Microsoft .NET Framework Version 2.0 und MMC Version 3.0 vorhanden sein, was in Windows 7 standardmäßig der Fall ist.
   - **Tools and templates** Dieses Feature installiert die Assistenten und die Vorlagen für Bereitstellungsdateien, etwa *Unattend.xml*. In der Standardeinstellung wird dieses Feature unter *C:\Program Files\Microsoft Deployment Toolkit* abgelegt.

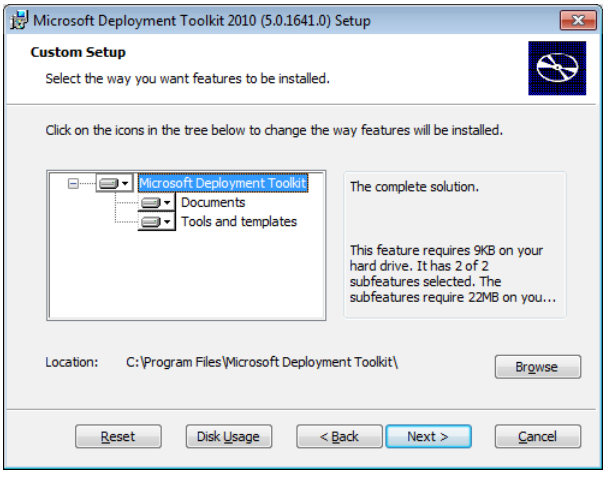

Microsoft Deployment Toolkit 2010 (5.0.1641.0) Setup
Custom Setup
Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.
Microsoft Deployment Toolkit
Documents
Tools and templates
The complete solution.
This feature requires 9KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 22MB on you...
Location:
C:\Program Files\Microsoft Deployment Toolkit\
Browse
Reset
Disk Usage
< Back
Next >
Cancel

Abbildung 3.35 Auswählen, welche MDT-Features installiert werden

6. Sie können den Status eines Features ändern, indem Sie es anklicken und den gewünschten Status auswählen. Den Zielordner ändern Sie, indem Sie *Microsoft Deployment Toolkit* auswählen und dann auf die Schaltfläche *Browse* klicken. Geben Sie im Dialogfeld *Change current destination folder* den neuen Zielordner an und klicken Sie auf *OK*.
7. Stellen Sie sicher, dass *Microsoft Deployment Toolkit* ausgewählt ist, wie oben in Abbildung 3.35 gezeigt, und klicken Sie auf *Install*. Klicken Sie auf *Ja*, falls Sie bestätigen müssen, dass das Programm ausgeführt werden darf.
8. Warten Sie, bis die Installation abgeschlossen ist, und klicken Sie dann auf *Finish*.

Übung 4 Erstellen einer Bereitstellungsfreigabe

In dieser Übung legen Sie eine Bereitstellungsfreigabe an. Sie müssen MDT 2010 installiert haben, bevor Sie diese Übung beginnen. Gehen Sie folgendermaßen vor, um eine Bereitstellungsfreigabe zu erstellen:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Klicken Sie im Startmenü auf *Alle Programme*, dann auf *Microsoft Deployment Toolkit* und schließlich auf *Deployment Workbench*. Klicken Sie auf *Ja*, falls Sie gefragt werden, ob Sie die Ausführung des Programms erlauben.

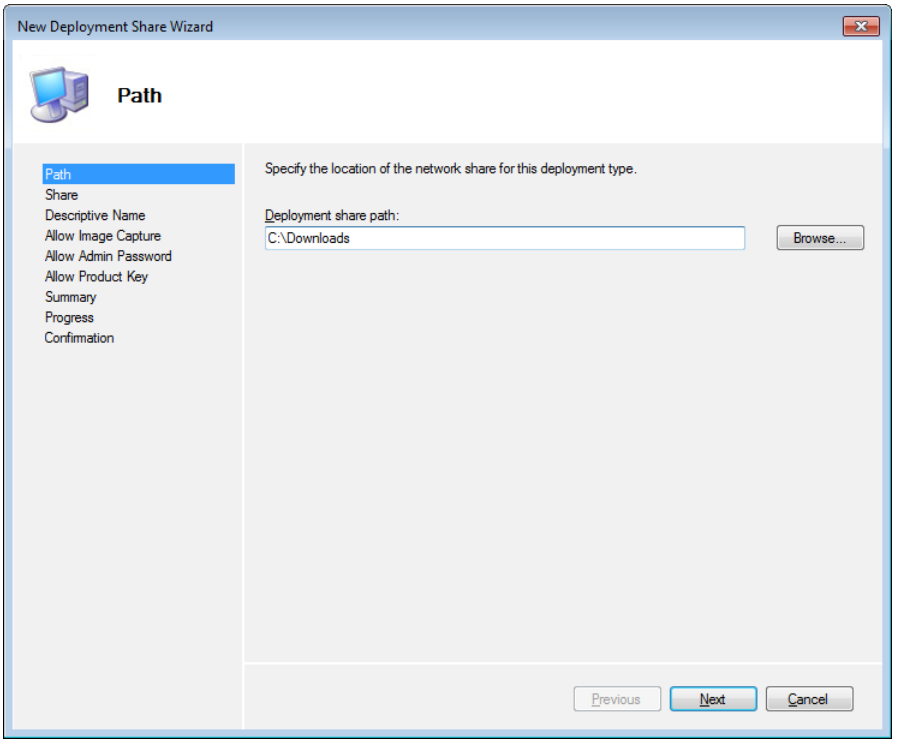


Abbildung 3.36 Angeben des Pfads für die Bereitstellungsfreigabe

3. Klicken Sie in der Deployment Workbench mit der rechten Maustaste auf *Deployment Shares* und wählen Sie den Befehl *New Deployment Share*, um eine neue Bereitstellungsfreigabe anzulegen.
4. Geben Sie auf der Seite *Path* des Assistenten in das Textfeld *Deployment share path* den Pfad **C:\Downloads** ein (Abbildung 3.36). Dies wird die neue Bereitstellungsfreigabe. Klicken Sie auf *Next*.
5. Geben Sie auf der Seite *Share* den Freigabenamen **Downloads$** ein und klicken Sie auf *Next*. Übernehmen Sie auf den folgenden Assistentenseiten die Standardeinstellungen und klicken Sie jeweils auf *Next*. Warten Sie, bis die Bereitstellungsfreigabe erstellt wurde, und schließen Sie den Assistenten dann mit *Finish*.
6. Wechseln Sie im Windows-Explorer in den Ordner *C:\Downloads* und prüfen Sie, ob die erforderlichen Unterordner angelegt wurden (Abbildung 3.37). Einige dieser Ordner (zum Beispiel *Applications*) sind anfangs leer, andere (etwa *Tools*) enthalten Dateien.

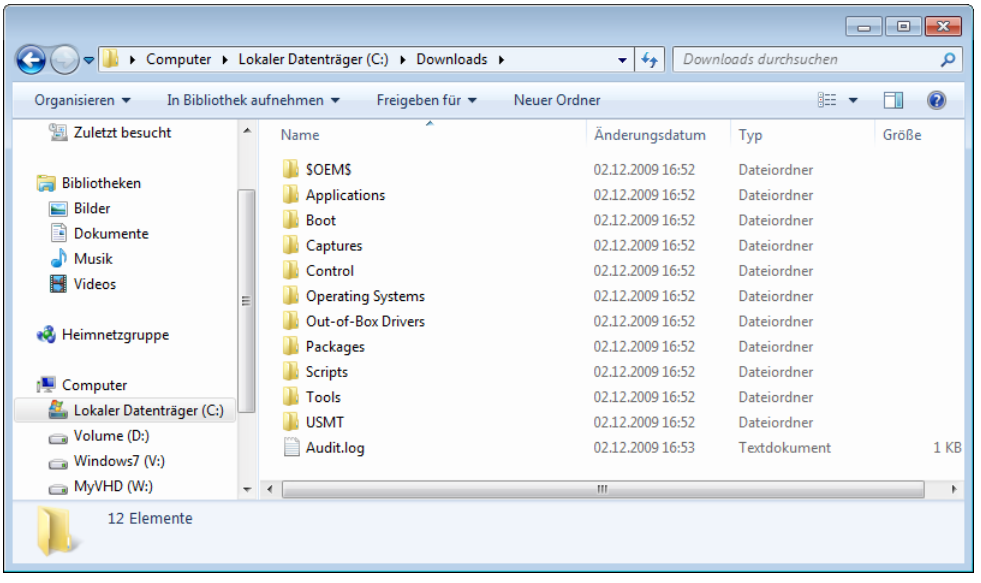


Abbildung 3.37 Inhalt einer neu erstellten Bereitstellungsfreigabe

Übung 5 Installieren eines Abbilds in der Bereitstellungsfreigabe

In dieser Übung installieren Sie die Windows 7-Quelldateien vom Windows 7-Installationsmedium in der Bereitstellungsfreigabe, die Sie in der vorherigen Übung angelegt haben. Gehen Sie folgendermaßen vor, um dieses Abbild zu installieren:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Legen Sie die Installations-DVD für die x86-Version von Windows 7 ein. Schließen Sie das Dialogfeld *Automatische Wiedergabe*, falls es sich öffnet. In dieser Übung hat das DVD-Laufwerk den Buchstaben *F:*. Falls Ihr Computer einen anderen Laufwerkbuchstaben verwendet, müssen Sie die folgenden Schritte entsprechend anpassen.
3. Öffnen Sie die Deployment Workbench.

4. Erweitern Sie unter *Deployment Workbench* die Knoten *Deployment Shares* und den Knoten Ihrer neu erstellten Bereitstellungsfreigabe *C:\Downloads*. Wählen Sie darin den Knoten *Operating Systems* aus.
5. Klicken Sie im Fensterabschnitt *Aktionen* auf *Import Operating System*, um ein Betriebssystem in die Bereitstellungsfreigabe zu importieren.
6. Stellen Sie sicher, dass auf der Seite *OS Type* des Assistenten die Option *Full set of source files* ausgewählt ist (Abbildung 3.38). Sie können stattdessen auch eine benutzerdefinierte Abbilddatei (Option *Custom image file*) verwenden, beispielsweise die Datei *Myimage.wim*, die Sie in Kapitel 2 aufgezeichnet und auf Ihrer startfähigen VHD bereitgestellt haben, oder ein WDS-Abbild, das auf einem angegebenen WDS-Server zur Verfügung steht.

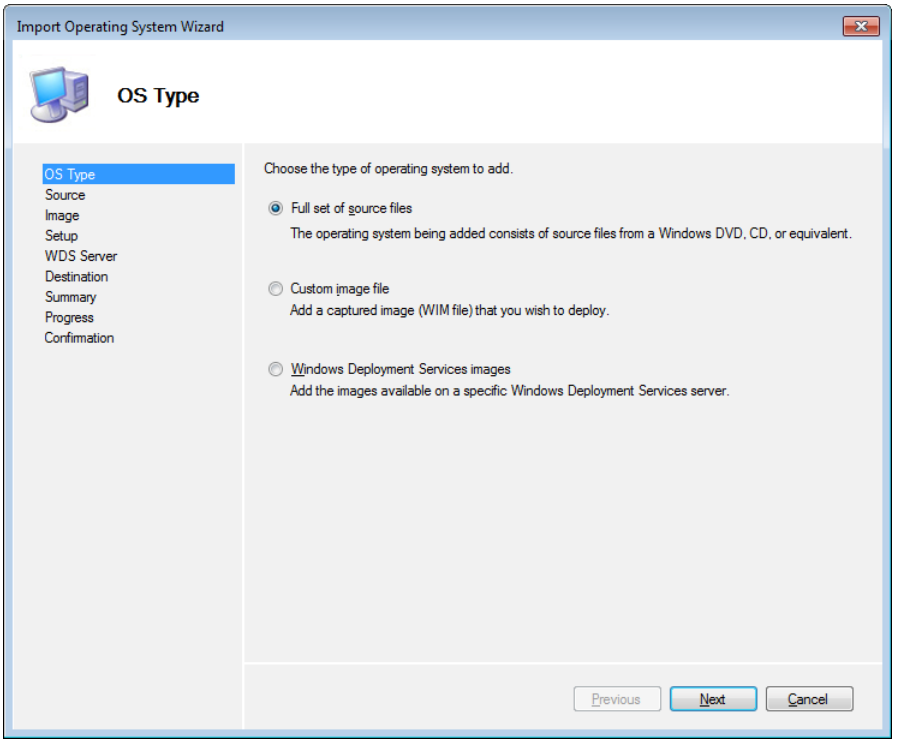


Abbildung 3.38 Auswählen eines vollständigen Satzes Quelldateien

7. Klicken Sie auf *Next*.
8. Geben Sie auf der Seite *Source* im Textfeld *Source directory* den Laufwerkbuchstaben **F:** als Quellverzeichnis ein. Klicken Sie auf *Next*.
9. Stellen Sie sicher, dass im Textfeld *Destination directory name* als Name des Zielverzeichnisses *Windows 7 x86* eingetragen ist. Klicken Sie auf zweimal auf *Next*.
10. Der Kopiervorgang dauert einige Zeit. Warten Sie, bis er abgeschlossen ist, schließen Sie den Assistenten mit *Finish* und prüfen Sie dann, ob die richtigen Betriebssystemabbilder in die Bereitstellungsfreigabe gelegt wurden (Abbildung 3.39).

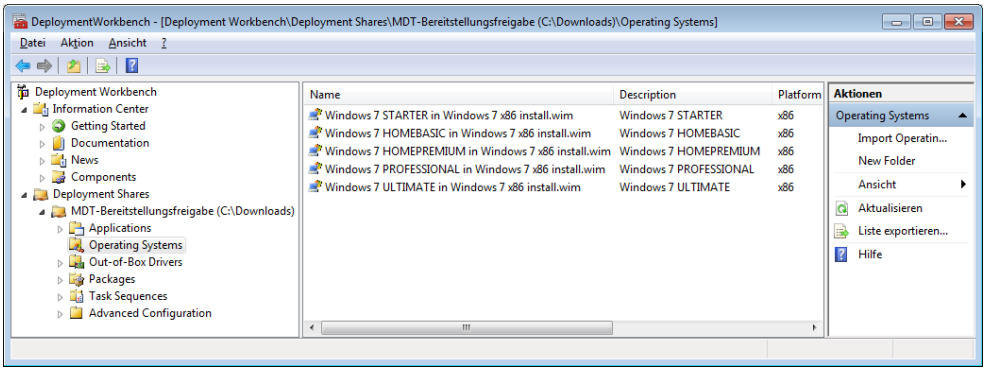


Abbildung 3.39 Betriebssystemabbilder wurden in die Bereitstellungsfreigabe gelegt

Zusammenfassung der Lektion

- Mit MDT 2010 können Sie Datenträgerabbilder verwalten und bearbeiten und eine Bereitstellungsfreigabe erstellen, über die Sie ein Betriebssystemabbild an andere Computer in Ihrem Netzwerk verteilen. Sie müssen das Windows AIK installieren, um WIM-Abbilddateien erstellen oder bereitstellen zu können.
- WDS verwendet Startabbilder, die es PXE-kompatiblen Computern ermöglichen, beim Start über das Netzwerk ein Installationsabbild abzurufen. Ist ein Computer nicht PXE-kompatibel, können Sie ihn mit einem Suchabbild starten, das auf einem startfähigen Medium gespeichert ist; WDS kann dann ein Installationsabbild auf dem Computer bereitstellen. Mithilfe von Aufzeichnungsabbildern können Sie einen Referenzcomputer starten und sein Systemabbild in WDS speichern, um es von dort aus auf anderen Computern bereitzustellen.
- MDT 2010 kann in einer LTI-Konfiguration mit WDS zusammenarbeiten. Damit MDT 2010 ZTI implementieren kann, müssen SCCM 2007 und SQL Server im Netzwerk verfügbar sein. MDT 2010 setzt außerdem immer voraus, dass das Windows AIK installiert ist.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Bereitstellen von Abbildern«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie wollen sicherstellen, dass VHD-Offlinedateien, die Installationen von Windows 7 enthalten, mit Service Packs und Softwareupdates auf dem neusten Stand gehalten werden. Welches Tool verwenden Sie dafür?

A. MDT 2010
B. Offline Virtual Machine Servicing Tool
C. BCDEdit
D. Configuration Manager 2007 R2

2. Sie wollen eine WIM-Abbilddatei bereitstellen, die Sie auf einem Windows 7-Referenzcomputer aufgezeichnet haben. Sie müssen das Quellverzeichnis angeben, in dem die WIM-Datei liegt, auswählen, ob Setup- oder Sysprep-Dateien benötigt werden, und die Datei dann in die Bereitstellungsfreigabe verschieben. Welches Tool eignet sich dafür?
   A. Der Assistent zur Abbildaufzeichnung der Windows-Bereitstellungsdienste, der in einem WDS-Aufzeichnungsabbild enthalten ist
   B. Der Tasksequenzerstellungs-Assistent, den Sie im Tasksequenz-Editor von SCCM 2007 starten
   C. Der Assistent für neue Bereitstellungsfreigaben (*New Deployment Share Wizard*), den Sie in der Konsole *Deployment Workbench* starten
   D. Der Assistent zum Importieren von Betriebssystemen (*Import Operating System Wizard*), den Sie in der MDT 2010-Konsole *Deployment Workbench* starten
3. WDS erstellt Installations-, Start-, Such- und Aufzeichnungsabbilder. Welches davon installieren Sie auf einem startfähigen Wechseldatenträger?
   A. Installationsabbild
   B. Startabbild (Standardstartabbild)
   C. Suchabbild
   D. Aufzeichnungsabbild
4. Was muss vorhanden sein, damit WDS installiert werden kann und in der Lage ist, Abbilder bereitzustellen? (Wählen Sie alle zutreffenden Antworten aus.)
   A. AD DS
   B. MDT 2010
   C. SQL Server
   D. SCCM 2007
   E. DHCP
   F. DNS
5. Sie haben eine startfähige DVD erstellt, die ein Windows PE-Abbild, das Tool ImageX und ein WIM-Abbild von Windows 7 Ultimate Edition enthält, das Sie auf einer Arbeitsstation in Ihrem SOHO-Netzwerk aufgezeichnet haben. Sie haben das Abbild mit ImageX auf einem anderen Computer installiert. Welches Tool verwenden Sie, um diesen Computer so zu konfigurieren, dass er das Abbild startet?
   A. BCDboot
   B. DISM
   C. BCDEdit
   D. ImageX

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Sie verwenden DISM oder ImageX, um ein Systemabbild im Dateisystem bereitzustellen und die Bereitstellung wieder aufzuheben. DISM fügt Pakete, Treiber und Updates zu einem bereitgestellten Abbild hinzu und ruft Informationen über online und offline bereitgestellte Systemabbilder ab. Mit DISM können Sie auch Windows PE-Abbilder im Dateisystem bereitstellen und bearbeiten.
- Mit MDT 2010 können Sie Datenträgerabbilder verwalten und bearbeiten und sie über eine Bereitstellungsfreigabe auf Zielcomputern bereitstellen. Sie müssen das Windows AIK installieren, um mit MDT 2010 Abbilder bereitstellen zu können.
- WDS erzeugt ein Systemstartmenü, in dem Sie auf einem PXE-kompatiblen Computer, der über das Netzwerk startet, ein Systemabbild auf dem Computer installieren können. Ist ein Zielcomputer nicht PXE-kompatibel, können Sie ihn von einem Suchabbild starten, um auf das Systemstartmenü zuzugreifen. Ein Aufzeichnungsabbild ist ein spezieller Typ Startabbild, das ebenfalls im Startmenü erscheint. Wenn Sie einen Referenzcomputer von einem Aufzeichnungsabbild starten, können Sie sein Systemabbild aufzeichnen und es auf einen WDS-Server kopieren, der es wiederum auf anderen Zielcomputern bereitstellt.
- Sie brauchen MDT 2010 (und das Windows AIK) sowie SCCM 2007 und SQL Server, um ZTI zu implementieren. Um LTI auf PXE-kompatiblen Computern zu implementieren, benötigen Sie MDT 2010 und WDS.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Startabbild**
- **Übernehmen von Änderungen**
- **Bereitstellen**
- **Bereitstellungsfreigabe**
- **Installationsabbild**
- **Bereitstellen im Dateisystem**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie an, was Sie über das Bereitstellen von Systemabbildern gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Bereitstellen eines Abbilds mit mehreren Language Packs

Don Hall, ein Systemadministrator bei Litware, hat ein primäres Bereitstellungsabbild für die Windows 7-Clientcomputer des Unternehmens erstellt. Er stellt fest, dass er ein Update einspielen, einen neuen Treiber hinzufügen, Einstellungen ändern und mehrere Sprachen unterstützen muss. Er möchte diese Änderungen durchführen, ohne das Abbild bereitstellen und erneut aufzeichnen zu müssen. Er weiß, dass er nicht das Tool Sysprep ausführen muss, wenn er das Abbild offline bearbeitet, und dass er daher nicht die Aktivierungsfrist zurücksetzen muss.

Litware ist ein relativ kleines Unternehmen mit zwei Niederlassungen. Diese zwei Niederlassungen befinden sich aber in unterschiedlichen Ländern. Don hat ein einziges Masterabbild erstellt, damit er nicht mehrere Varianten verwalten muss. Dieses Abbild enthält beide Language Packs, die bei Litware gebraucht werden. Don muss Updates auf dieses eine Abbild anwenden und sicherstellen, dass alle Updates auf alle Sprachen im Abbild angewendet werden. Bevor er das Abbild bereitstellt, löscht er im Rahmen einer Offlinewartung das nicht benötigte Language Pack. Er braucht nur das Windows 7-Abbild von Litware zu pflegen. Es ist nicht nötig, eine Wartung für das Windows PE-Abbild durchzuführen.

Don hat vor, das Offlineabbild mit dem Tool DISM im Dateisystem bereitzustellen und es zu bearbeiten, die Bereitstellung des Abbilds im Dateisystem dann wieder aufzuheben und die Änderungen zu übernehmen. Außerdem will er DISM einsetzen, um einen Bericht über den Status von Treibern, Anwendungen, Spracheinstellungen und installierten Paketen zu erstellen.

1. Was braucht Don, um diese Aufgaben zu erledigen?
2. Was muss Don als Erstes mit dem Masterabbild machen?
3. Welche Aufgaben führt Don mit dem Tool DISM aus?

Übung mit Fallbeispiel 2: Bereitstellen eines Abbilds auf 100 Clientcomputern

Sie sind Netzwerkadministrator bei Northwind Traders. Ihr Unternehmen baut die Niederlassung Detroit von einer kleinen Zweigstelle zu einer großen Niederlassung aus, und Sie haben die Aufgabe, 100 Clientcomputer bereitzustellen. Die Serverinfrastruktur wurde bereits aufgerüstet. Detroit ist Teil der AD DS-Domäne von Northwind Traders, und im dortigen Subnetz stehen DHCP- und DNS-Server zur Verfügung. Auf einem Mitgliedserver, der unter Windows Server 2008 R2 läuft, wurde die WDS-Serverrolle installiert und konfiguriert, außerdem wurde ein Standardstartabbild erstellt.

Sie haben eine Arbeitsstation mit Windows 7 Enterprise erhalten, die vorher von einem Angestellten benutzt wurde, der das Unternehmen inzwischen verlassen hat. Alle persönlichen Dateien und unwichtigen Anwendungen wurden vom Computer gelöscht. Ihr Chef will, dass

alle neuen Clientcomputer »genau wie der hier« installiert werden. Die Zielcomputer wurden neu gekauft und erfüllen problemlos die empfohlenen Spezifikationen für Windows 7 Enterprise. Sie sind PXE-kompatibel.

1. Was müssen Sie mit der Arbeitsstation machen, die Sie erhalten haben, bevor Sie sie als Referenzcomputer verwenden können?
2. Was müssen Sie in WDS erstellen, damit Sie ein Abbild des Referenzcomputers aufzeichnen können?
3. Wie führen Sie die Bereitstellung der Zielcomputer durch?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Verwalten und Bearbeiten eines Systemabbilds

Arbeiten Sie diese Übung durch, während Sie unter dem Benutzerkonto *Kim_Akers* am Computer *Canberra* angemeldet sind.

- Verwenden Sie das Tool DISM. Wie alle Befehlszeilentools sieht es erst hochkompliziert aus, mit etwas Übung wird es aber schnell vertraut. Stellen Sie das Abbild auf Ihrer startfähigen VHD im Dateisystem bereit, rufen Sie mit allen `Get`-Befehlen Informationen ab und versuchen Sie dann, alle Konfigurationsbefehle auszuführen. Übernehmen Sie Ihre Änderungen in das Abbild, starten Sie von der VHD und sehen Sie sich das Ergebnis Ihrer Änderungen an.

Machen Sie sich mit den Bereitstellungstools vertraut

Arbeiten Sie die erste Übung durch, während Sie unter dem Benutzerkonto *Kim_Akers* am Computer *Canberra* angemeldet sind. Die zweite und dritte Übung sind optional.

- **Übung 1** MDT ist bereits auf dem Computer *Canberra* installiert. Verwenden Sie das Tool, um ein Betriebssystemabbild, Treiber, Updates, Language Packs und Anwendungen zu installieren. Erstellen und bearbeiten Sie Tasksequenzen und verknüpfen Sie Antwortdateien mit dem Abbild.
- **Übung 2** Erstellen Sie einen virtuellen PC, der unter Windows 7 läuft. Stellen Sie das Systemabbild bereit, das Sie in MDT erstellt haben, und sehen Sie sich die Auswirkungen an.
- **Übung 3** Erstellen Sie einen virtuellen Server, der unter Windows Server 2008 läuft. Installieren Sie die AD DS-Serverrolle und konfigurieren Sie DHCP und DNS. Installieren Sie die WDS-Serverrolle und üben Sie die Arbeit mit der Konsole *Windows-Bereitstellungsdienste* und dem Befehlszeilentool WDSUTIL.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

KAPITEL 4

Verwalten von Geräten und Datenträgern

Dieses Kapitel beschäftigt sich mit zwei Themen, die für den typischen Benutzer von besonderer Bedeutung sind. Die Benutzerzufriedenheit hängt stark davon ab, wie gut Peripheriegeräte und interne Komponenten funktionieren. Es ist Ihre Aufgabe sicherzustellen, dass die besten verfügbaren Gerätetreiber auf den Clientcomputern der Organisation installiert sind. Nicht immer ist der neuste Treiber auch der beste, daher müssen Sie sicherstellen, dass die neusten Gerätetreiber, die von einer Updatesite (üblicherweise Windows Update) heruntergeladen werden, auch zu Ihrer Hardware kompatibel sind, bevor Sie sie für Ihre Netzwerkclients bereitstellen.

Wenn die Festplatte auf einem Clientcomputer stark fragmentiert ist, Defekte hat, zu wenig Platz darauf frei ist oder Sie die Datenträgersysteme nicht für optimale Leistung oder Fehlertoleranz konfiguriert haben, sinkt die Benutzerzufriedenheit schlagartig. Ihnen stehen für die Verwaltung von Datenträgern sowohl Programme mit grafischer Benutzeroberfläche (Graphical User Interface, GUI) als auch Befehlszeilentools zur Verfügung. Mithilfe dieser Tools stellen Sie sicher, dass die Datenträger optimale Leistung bieten. Falls Ihre Clientcomputer mehrere Festplatten enthalten, müssen Sie außerdem sicherstellen, dass die Laufwerkarrays richtig konfiguriert sind.

Dieses Kapitel beschreibt die Tools und Techniken, mit denen Sie Geräte und Gerätetreiber sowie Datenträger verwalten.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von Geräten
- Verwalten von Datenträgern

Lektionen in diesem Kapitel:

- Lektion 1: Verwalten von Gerätetreibern und Geräten 193
- Lektion 2: Verwalten von Datenträgern 225

Bevor Sie beginnen

Um die Übungen in diesem Kapitel durchzuarbeiten, müssen Sie folgende Vorbereitungen getroffen haben:

- Sie haben Windows 7 auf einem eigenständigen Client-PC installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben. Sie brauchen Internetzugriff, um die Übungen durchzuführen. Außerdem brauchen Sie ein USB-Flashspeichergerät (Universal Serial Bus), um die Übungen in Lektion 2 durchzuarbeiten.

Praxistipp

Ian McLean

Die meisten Benutzer wollen nichts mit der internen Funktionsweise ihrer Computer zu tun haben. Selbst der kleine Anteil der Benutzer, die wissen, was ein Motherboard ist, denkt selten darüber nach, welche Funktion es hat. Viel mehr Aufmerksamkeit schenken Benutzer den diversen Geräten. Funktioniert die Tastatur richtig oder erscheint ein Anführungszeichen, wenn sie die Taste Ö drücken? Ist der Bildschirm scharf, klar und einfach abzulesen und ist die Bildschirmauflösung optimal? Arbeitet die Maus? Ist der Datenträgerzugriff zu langsam? Ist auf einem USB-Flashstick eine wichtige Datei verloren gegangen und kann jemand anders die Daten auf dem Flashspeichergerät lesen, das der CEO im Flugzeug vergessen hat? Die Liste ist endlos.

Sowohl Administratoren als auch Helpdeskmitarbeiter verbringen viel Zeit mit Problemen, die sich um Peripheriegeräte drehen. Wenn ein Motherboard ausfällt, tauschen Sie es aus. Aber mit der Konfiguration von Geräten, die Benutzer an ihren Computer anschließen wollen, oder von Druckern, die im Prinzip funktionieren, aber nicht ganz so, wie es der Benutzer erwartet, können Sie unter Umständen endlos viele Stunden verbringen. Ein großer Teil der Updates, die Sie anwenden, enthalten aktualisierte Treiber. Und manchmal funktioniert ein neuer Treiber nicht so gut wie der alte, oder er verursacht Konflikte mit anderen Treibern eines Computers. Wie oft haben Sie den Satz gehört: »Das Dings, das an meinen Computer angesteckt ist, funktioniert nicht mehr; seit Sie damit rumgespielt haben, geht es nicht mehr richtig«?

Zu Ihren Aufgaben gehört es, grundlegende technische Probleme auf wichtiger Hardware wie Domänencontrollern und Servern zu beseitigen, die Microsoft SQL Server oder Microsoft Exchange Server ausführen. Aber Sie verbringen auch viel Zeit mit Geräten, Gerätetreibern, Druckern und diesen widerspenstigen Peripheriegeräten. Letztlich besteht Ihr wichtigstes Ziel darin, dass die Benutzer zufrieden sind.

Lektion 1: Verwalten von Gerätetreibern und Geräten

In dieser Lektion erfahren Sie, wie Sie herausfinden, welcher Treiber ein Peripheriegerät steuert, und wie Sie prüfen, ob er richtig funktioniert. Sie lernen, wie Sie einen Gerätetreiber aktualisieren, deaktivieren oder deinstallieren und wie Sie die vorherige Treiberversion wiederherstellen, falls ein vor Kurzem installierter Treiber nicht funktioniert (und beispielsweise Abbruchfehler verursacht). Die Lektion beschäftigt sich mit signierten Treibern, Konflikten zwischen Treibern, der Konfiguration von Treibereinstellungen und dem Beseitigen von Gerätetreiberproblemen. Vor allem arbeiten Sie dabei mit der Konsole *Geräte-Manager*, dem Tool, das Windows 7 für die Verwaltung von Geräten und Gerätetreibern zur Verfügung stellt.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Installieren von Plug & Play- (PnP) und Nicht-PnP-Hardware
- Aktualisieren, Deaktivieren und Deinstallieren eines Gerätetreibers und Wiederherstellen der Vorversion eines Treibers
- Vorabbereitstellen eines Gerätetreibers und Erlauben, dass Standardbenutzer Geräte installieren, die zu einem bestimmten Geräteinstallationstyp gehören
- Konfigurieren von Treiberupdates von der Windows Update-Website
- Beseitigen von Problemen mit Gerätetreibern

Veranschlagte Zeit für diese Lektion: 50 Minuten

Anzeigen von Geräteinformationen im Geräte-Manager

Ein Gerätetreiber ist ein Softwarepaket (normalerweise eine *.exe*-Datei, die von einer *.inf*-Datei installiert wird), das es Windows 7 ermöglicht, mit einem bestimmten Hardwaregerät zu kommunizieren. Damit Windows 7 neue Hardware benutzen kann, muss ein Gerätetreiber für diese Hardware installiert werden. Falls das Gerät Plug & Play-fähig (PnP-fähig) ist, müsste der Treiber automatisch installiert werden, aber unter Umständen müssen Sie später aktualisierte Treiber installieren, wenn sie veröffentlicht und heruntergeladen werden. Wird der Treiber nicht automatisch installiert, müssen Sie ihn selbst installieren. Im Geräte-Manager können Sie Treiber für Hardwaregeräte installieren und aktualisieren, die Hardwareeinstellungen für Geräte ändern und Probleme beseitigen.

Im Geräte-Manager erledigen Sie folgende Arbeiten:

- Ermitteln, welche Gerätetreiber für ein Gerät geladen sind, und Abrufen von Informationen über alle Gerätetreiber
- Feststellen, ob die Hardware Ihres Computers und die zugehörigen Gerätetreiber einwandfrei funktionieren
- Auflisten der Geräte anhand ihres Typs, anhand der Verbindung zum Computer oder anhand der benutzten Ressourcen
- Aktivieren, Deaktivieren und Deinstallieren von Geräten
- Ändern von Hardwarekonfigurationseinstellungen
- Installieren von aktualisierten Gerätetreibern
- Wiederherstellen der Vorgängerversion eines Treibers

- Ändern erweiterter Einstellungen und Eigenschaften für Geräte
- Anzeigen ausgeblendeter Geräte

Meist verwenden Sie den Geräte-Manager, um den Status Ihrer Hardware zu überprüfen und Gerätetreiber auf einem Clientcomputer zu aktualisieren. Außerdem können Sie mit den Diagnosefeatures des Geräte-Managers Gerätekonflikte auflösen und Ressourceneinstellungen ändern. Allerdings weist das System die Ressourcen während des Hardwaresetups automatisch zu und Sie brauchen die Ressourceneinstellungen nur selten zu ändern (wenn es überhaupt möglich ist).



Hinweis Der Geräte-Manager arbeitet auf einem Remotecomputer im reinen Lesemodus

Sie können mit dem Geräte-Manager nur Geräte und Treiber des lokalen Computers verwalten. Auf einem Remotecomputer arbeitet der Geräte-Manager im reinen Lesemodus, daher ist es nicht möglich, die Hardwarekonfiguration eines solchen Computers zu ändern.

Starten des Geräte-Managers

Sie können den Geräte-Manager auf einem Windows 7-Computer unabhängig davon öffnen, unter welchem Konto Sie angemeldet sind. In der Standardeinstellung dürfen allerdings nur Administratoren Änderungen an Geräten vornehmen und Treiber installieren, deinstallieren und die Vorversion wiederherstellen.

Es gibt folgende Möglichkeiten, den Geräte-Manager zu öffnen:

- Klicken Sie in der Systemsteuerung auf *Hardware und Sound*. Klicken Sie dann unter *Geräte und Drucker* auf *Geräte-Manager*.
- Klicken Sie im Startmenü mit der rechten Maustaste auf *Computer* und wählen Sie den Befehl *Verwalten*. Klicken Sie in der Konsolenstruktur von *Computerverwaltung* auf *Geräte-Manager*.
- Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben Sie **mmc devmgmt.msc** ein. Wenn Sie die Eingabeaufforderung nicht als Administrator ausführen, wird der Geräte-Manager im reinen Lesemodus gestartet.

Sie können den Geräte-Manager auch auf einem Remotecomputer starten. Öffnen Sie die Computerverwaltung und wählen Sie im Menü *Aktion* den Befehl *Verbindung mit anderem Computer herstellen*. Geben Sie entweder den Namen des Remotecomputers ein oder klicken Sie auf *Durchsuchen* und wählen Sie ihn aus. Klicken Sie auf *OK*. Nun können Sie sich im Geräte-Manager die Geräte und Geräteeinstellungen auf dem Remotecomputer ansehen. Es ist allerdings nicht möglich, Einstellungen zu ändern oder Treiber zu installieren, zu deinstallieren oder die Vorversion eines Treibers wiederherzustellen.

Unabhängig davon, welche Methode Sie wählen, öffnet sich der Geräte-Manager mit der Ansicht, die in Abbildung 4.1 zu sehen ist. Wenn Sie die Computerverwaltung verwenden, befindet sich auf der linken Seite zusätzlich die Konsolenstruktur von *Computerverwaltung*.



Hinweis Starten des Geräte-Managers

In den Übungen weiter unten in dieser Lektion werden Sie aufgefordert, den Geräte-Manager zu öffnen. Dabei ist es egal, welche Methode Sie wählen. Sie brauchen den Geräte-Manager in diesen Übungen nicht auf einem Remotecomputer zu öffnen.

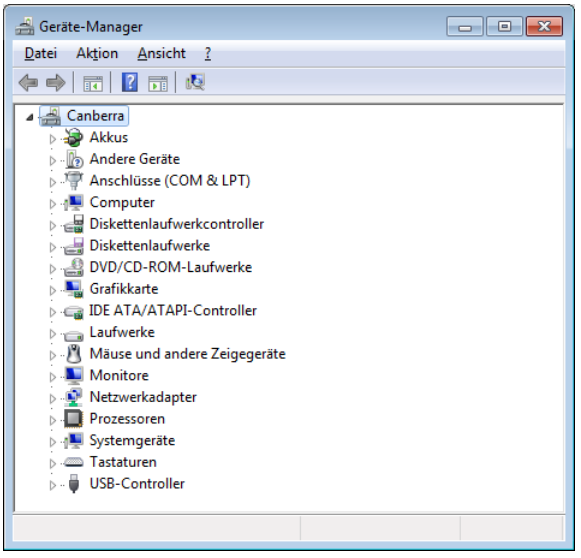


Abbildung 4.1 Der Geräte-Manager

Anzeigen von Geräteinformationen

Sie können sich im Geräte-Manager den Status und Details von Geräten ansehen (auch von ausgeblendeten Geräten), den Stromverbrauch und die Bandbreitenzuweisung für ein USB-Gerät überwachen und Gerätetreiberinformationen anzeigen.

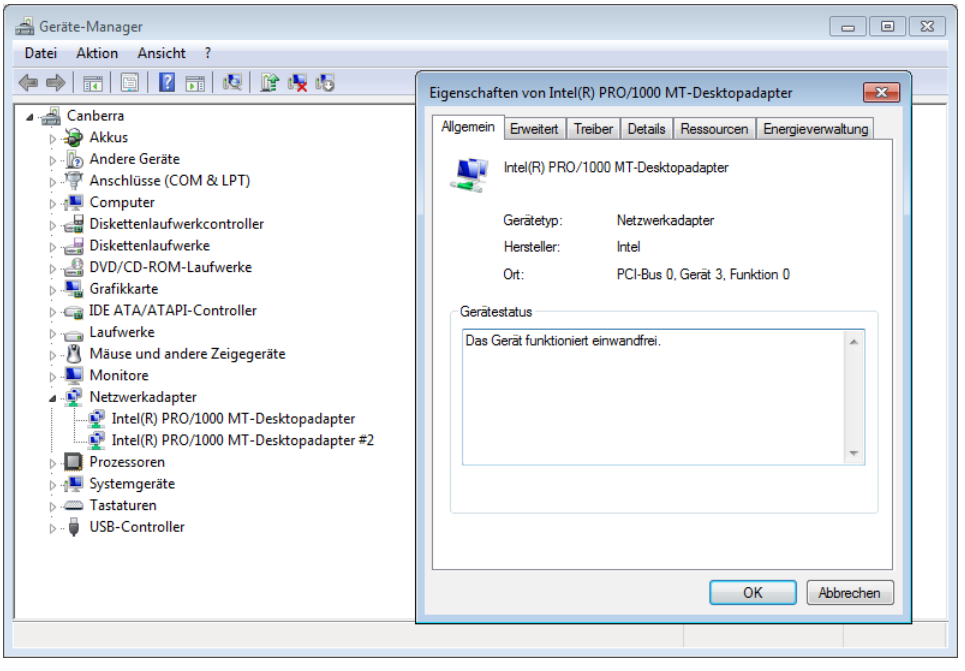


Abbildung 4.2 Anzeigen des Gerätestatus

Den Status eines Geräts sehen Sie, indem Sie doppelt auf den Typ des gewünschten Geräts klicken (Tastaturen, Monitore, Netzwerkadapter und so weiter), dann mit der rechten Maustaste auf das Gerät klicken und den Befehl *Eigenschaften* wählen. Auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds ist im Abschnitt *Gerätestatus* angegeben, ob das Gerät einwandfrei funktioniert. Ist das der Fall, ist ein Treiber installiert und Windows 7 kann damit kommunizieren. Abbildung 4.2 zeigt den Status eines Netzwerkadapters.

Tritt bei dem Gerät ein Problem auf, wird die Art des Problems angezeigt. Zusätzlich erhalten Sie manchmal einen Problemcode und eine Nummer sowie einen Lösungsvorschlag. Falls die Schaltfläche *Nach Lösungen suchen* sichtbar ist, können Sie einen Windows-Fehlerbericht an Microsoft senden.

Auf der Registerkarte *Energieverwaltung* konfigurieren Sie Einstellungen, die festlegen, ob das Gerät deaktiviert werden kann, um Strom zu sparen, und ob es den Computer aufwecken darf (nur bei bestimmten Netzwerkadaptern mithilfe eines speziellen Pakets). Das spezielle Paket (magic packet) ist ein Standardframe zum Aufwecken des Computers über LAN, der an eine bestimmte Netzwerkschnittstelle gerichtet ist und den Remotezugriff auf einen Computer ermöglicht, der sich im Energiesparmodus befindet.



Hinweis **Unterschiedliche Geräte haben unterschiedliche Registerkarten**

Nicht bei allen Geräten gibt es die Registerkarten *Erweitert* und *Energieverwaltung*. Im Allgemeinen haben Netzwerkgeräte wie Bus-Hostcontroller und Netzwerkadapter eine *Energieverwaltung*-Registerkarte, allerdings gibt es nur bei Netzwerkadaptern die Möglichkeit, den Computer aus dem Ruhezustand aufzuwecken. Datenträgercontroller haben Registerkarten namens *Richtlinien* und *Volumes*. Alle Geräte haben die Registerkarten *Allgemein*, *Treiber* und *Details*. Sind einem Gerät Ressourcen zugewiesen, hat es außerdem die Registerkarte *Ressourcen*.

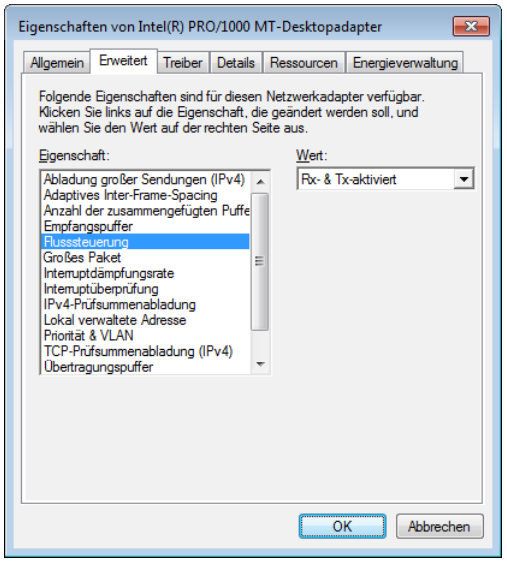


Abbildung 4.3 Erweiterte Einstellungen

Die Registerkarte *Ressourcen* enthält Details zum Arbeitsspeicherbereich, zu den IRQs (Interrupt Request) und zu dem E/A-Bereich (Ein-/Ausgabe), die von dem Gerät benutzt werden. Auf der Registerkarte *Erweitert* (Abbildung 4.3) haben Sie Zugriff auf eine Reihe konfigurierbarer Einstellungen. Welche das sind, hängt vom Typ des Geräts ab, dessen Eigenschaftendialogfeld Sie anzeigen. Die Registerkarte *Details* (Abbildung 4.4) zeigt sogar noch mehr Eigenschaften an. Sie können darin jede Eigenschaft anklicken und sich ihren Wert ansehen. Die Registerkarte *Treiber* wird weiter unten in dieser Lektion beschrieben.

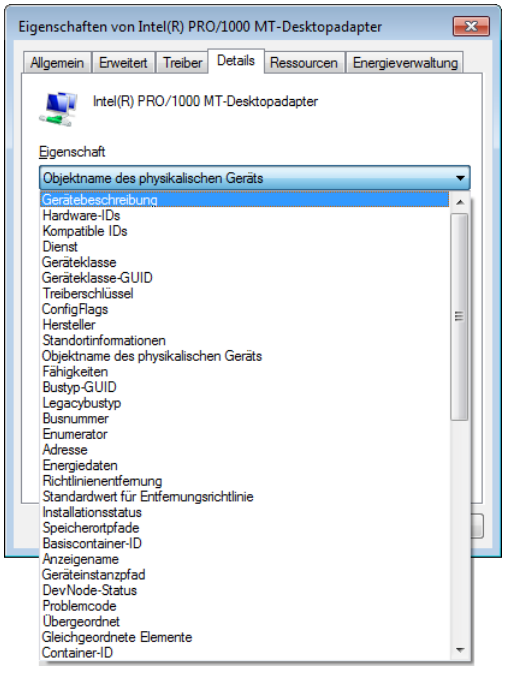


Abbildung 4.4 Details eines Netzwerkadapters

In der Standardeinstellung werden Geräte in der Anzeige nach ihrem Typ zu Gruppen zusammengefasst. Stattdessen können Sie sie auch danach sortieren, wie sie mit dem Computer verbunden sind, also beispielsweise in welchen Bus sie eingesteckt sind. Sie können sich die Ressourcen anhand des Typs des Geräts auflisten lassen, das die Ressource benutzt, oder nach dem zugewiesenen Verbindungstyp. Im Menü *Ansicht* des Geräte-Managers finden Sie Befehle, um in diese Ansichten umzuschalten.

Im Menü *Ansicht* können Sie auch ausgeblendete Geräte sichtbar machen. Normalerweise ist ein Gerät ausgeblendet, wenn es momentan nicht angeschlossen ist, aber Treiber dafür installiert sind. Das sind beispielsweise ältere Geräte und Geräte, die nicht mehr installiert sind. Abbildung 4.5 zeigt diese Ansicht.

Anzeigen des Stromverbrauchs für einen USB-Hub

Manche USB-Hubs haben eine eigene Stromversorgung (aktive Hubs), andere beziehen ihren Strom über den Bus (passive Hubs). Ein Hub mit eigener Stromversorgung wird über ein Netzteil versorgt, während ein passiver Hub den benötigten Strom über den USB bezieht,

an den er angeschlossen ist. Geräte, die viel Strom brauchen, etwa Kameras, sollten an Hubs mit eigener Stromversorgung angesteckt werden.

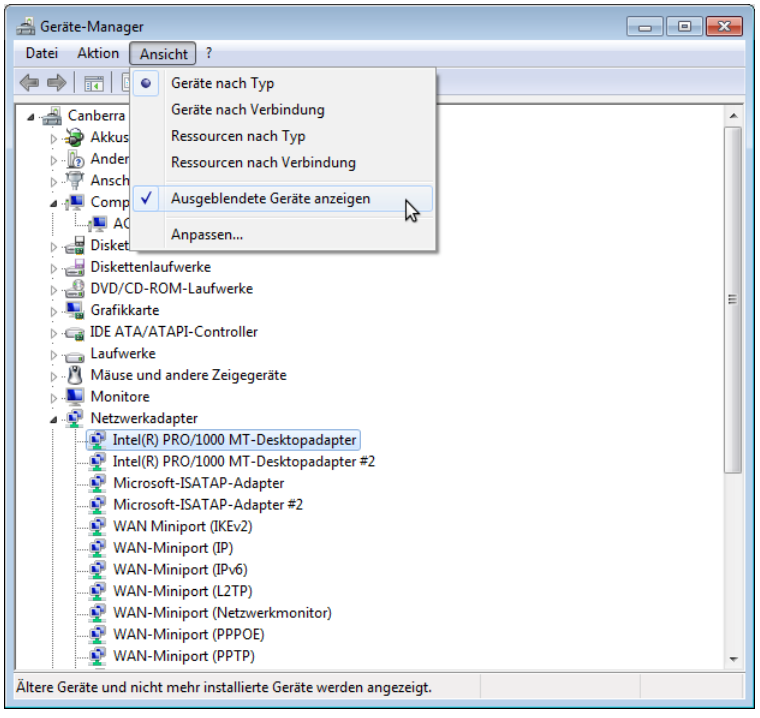


Abbildung 4.5 Anzeigen ausgeblendeter Geräte

Sie können den Stromverbrauch für einen USB-Hub prüfen, um Fälle zu erkennen, wo zu viele Geräte den Hub benutzen. Klicken Sie im Geräte-Manager doppelt auf den Knoten *USB-Controller*, klicken Sie mit der rechten Maustaste auf einen USB-Root-Hub und wählen Sie den Befehl *Eigenschaften*. Auf der Registerkarte *Stromversorgung* ist in der Liste *Angeschlossene Geräte* angegeben, wie viel Strom jedes Gerät verbraucht. Beachten Sie, dass der Eintrag *USB-Root-Hub* nur dann im Knoten *USB-Controller* erscheint, wenn Sie mindestens einen USB-Hub mit Ihrem Computer verbunden haben. Manche USB-Geräte (zum Beispiel Modems) werden nicht aufgeführt, weil sie keine Bandbreitenanforderungen an das Betriebssystem melden.

Anzeigen des Bandbreitenverbrauchs für einen USB-Hostcontroller

Jeder USB-Controller hat eine begrenzte Bandbreite, die sich alle angeschlossenen Geräte teilen. Falls Sie vermuten, dass ein USB-Controller mehr Bandbreite benötigt, können Sie das überprüfen, indem Sie anzeigen lassen, wie viel Bandbreite jedes Gerät momentan belegt. Klicken Sie im Geräte-Manager doppelt auf den Knoten *USB-Controller*, klicken Sie mit der rechten Maustaste auf den Hostcontroller Ihres Systems und wählen Sie den Befehl *Eigenschaften*. Auf der Registerkarte *Erweitert* wird in der Liste *Geräte, die Bandbreite verwenden* angezeigt, wie viel Bandbreite jedes Gerät belegt.

Anzeigen von Informationen über Gerätetreiber

Sie erhalten Details über die Gerätetreiber, die auf Ihrem Computer laufen, wenn Sie das Gerät auswählen, dessen Treiber Sie untersuchen wollen, mit der rechten Maustaste darauf klicken und den Befehl *Eigenschaften* wählen. Auf der Registerkarte *Treiber* können Sie auf *Treiber aktualisieren* klicken, um ein Update des Treibers durchzuführen, auf *Deinstallieren* klicken, um den Treiber zu entfernen, oder auf *Deaktivieren*, um das Gerät zu deaktivieren. Hat der aktuelle Treiber einen vorher installierten Treiber ersetzt, ist außerdem die Schaltfläche *Vorheriger Treiber* aktiviert. Einzelheiten über den Treiber erfahren Sie, indem Sie auf *Treiberdetails* klicken. Daraufhin öffnet sich das Dialogfeld *Treiberdateidetails* (Abbildung 4.6), in dem die einzelnen Dateien, aus denen der Treiber besteht, sowie Angaben zur Dateiversion und zur digitalen Signatur aufgelistet sind.

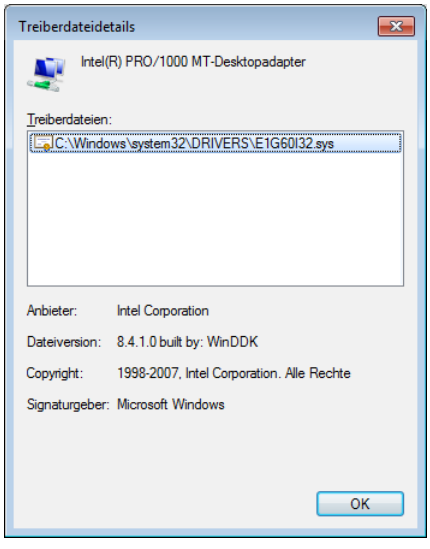


Abbildung 4.6 Treiberdetails

Installieren von Geräten und Verwalten von Gerätetreibern

PnP-Spezifikationen definieren, wie ein Computer neu hinzugefügte Hardware erkennt und konfiguriert und wie er automatisch den passenden Gerätetreiber installiert. Windows 7 unterstützt PnP. Wenn ein Benutzer ein Hardwaregerät ansteckt, sucht das Betriebssystem daher nach einem geeigneten Gerätetreiberpaket und konfiguriert es automatisch so, dass keine Konflikte mit anderen Geräten entstehen. Das macht die Installation sehr einfach.

Allerdings sollte Benutzern nicht erlaubt sein, beliebige Geräte an ihre Arbeitscomputer anzuschließen. Gerätetreibersoftware läuft quasi als Teil des Betriebssystems und hat uneingeschränkten Zugriff auf den gesamten Computer, daher sollten nur autorisierte Gerätetreiber erlaubt werden.

Wenn ein Benutzer ein Gerät ansteckt, erkennt Windows 7 die neue Hardware, und der Plug & Play-Dienst identifiziert das Gerät und sucht im Treiberspeicher nach einem Treiberpaket, das zum Gerät passt. Wird ein geeigneter Treiber gefunden, wird das Gerät als autorisiert eingestuft, und der Plug & Play-Dienst kopiert die Treiberdatei (oder Dateien) aus dem Treiberspeicher in den endgültigen Speicherort, normalerweise *C:\Windows\System32*

Drivers. Schließlich konfiguriert der Plug & Play-Dienst die Registrierung und startet den neu installierten Treiber.

Installieren von Gerätetreibern aus Windows Update

In der Standardeinstellung werden aktualisierte Gerätetreiber, die in Windows Update veröffentlicht werden, automatisch heruntergeladen und auf einem Clientcomputer installiert. Sie können dieses Verhalten im Dialogfeld *Geräteinstallationseinstellungen* anpassen (Abbildung 4.7). Am einfachsten öffnen Sie dieses Dialogfeld, indem Sie im Suchfeld des Startmenüs **Geräteinstallation** eingeben und dann auf *Geräteinstallationseinstellungen ändern* klicken.

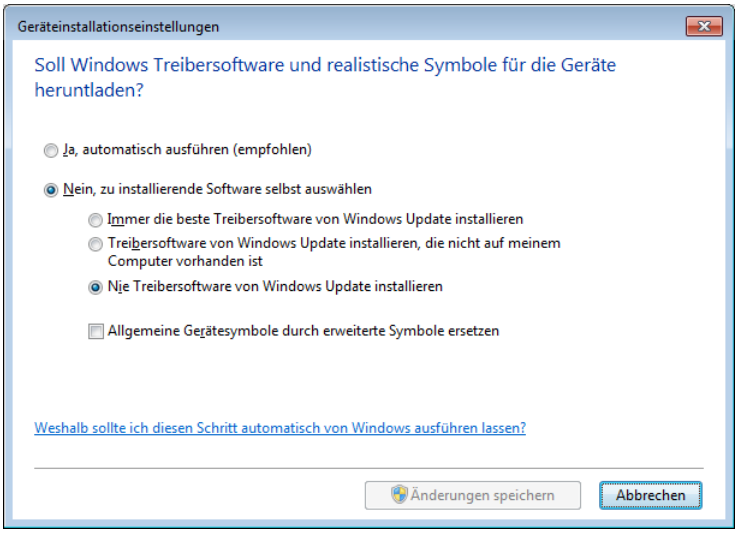

Geräteinstallationseinstellungen
Soll Windows Treibersoftware und realistische Symbole für die Geräte heruntladen?
Ja, automatisch ausführen (empfohlen)
Nein, zu installierende Software selbst auswählen
Immer die beste Treibersoftware von Windows Update installieren
Treibersoftware von Windows Update installieren, die nicht auf meinem Computer vorhanden ist
Nie Treibersoftware von Windows Update installieren
Allgemeine Gerätesymbole durch erweiterte Symbole ersetzen
Weshalb sollte ich diesen Schritt automatisch von Windows ausführen lassen?
Änderungen speichern
Abbrechen

Abbildung 4.7 Das Dialogfeld *Geräteinstallationseinstellungen*

Die Standardeinstellung ist *Ja, automatisch ausführen (empfohlen)*. Wollen Sie allerdings sicherstellen, dass nur Gerätetreiber, die Sie getestet haben, auf den Windows 7-Computern in Ihrer Organisation installiert werden, sollten Sie *Nie Treibersoftware von Windows Update installieren* auswählen.

Wenn Sie die Option *Immer die beste Treibersoftware von Windows Update installieren* auswählen, stellt Windows 7 automatisch fest, ob ein neuer Treiber besser ist als ein bereits installierter. Allerdings können Sie den neuen Treiber auf diese Weise nicht testen, bevor er installiert wird. Auch wenn Sie die Option *Treibersoftware von Windows Update installieren, die nicht auf meinem Computer vorhanden ist* auswählen, können Sie die neuen Treiber nicht testen, bevor sie installiert sind. In einer Unternehmensumgebung, insbesondere wenn Software mit Windows Server Update Services (WSUS) verteilt wird, sollten Treiberupdates von der Windows Update-Site deaktiviert und die Site aus dem Suchpfad gelöscht werden.

Staging eines Gerätetreibers

Liegt kein Gerätetreiber im Treiberspeicher vor, muss ein Administrator das Gerät genehmigen. Dieser Prozess wird als *Staging* bezeichnet. Sie können eine Computergruppenrichtlinie so konfigurieren, dass normale Benutzer die Installation eines Geräts genehmigen dürfen, sofern es zu einer bestimmten Gerätesetupklasse gehört. Oder Sie stellen einen geeigneten

Gerätetreiber bereit, sodass jeder Benutzer das Gerät installieren kann. Es wäre aber fahrlässig, das für alle Geräte zu machen. Wie Sie Gruppenrichtlinien konfigurieren, die es Nicht-Administratoren erlauben, ausgewählte Geräte und Gerätesetupklassen zu installieren, erfahren Sie in den Übungen weiter unten in dieser Lektion.

Windows 7 leitet den Stagingprozess dadurch ein, dass es in den Ordnern, die im Registrierungseintrag *DevicePath* angegeben sind, nach einem passenden Treiberpaket sucht. Wie Sie Windows 7 so konfigurieren, dass es in weiteren Ordnern nach Gerätetreibern sucht, erfahren Sie in den Übungen weiter unten in dieser Lektion. Wird kein geeigneter Treiber gefunden, sucht Windows 7 auf der Windows Update-Website. Schlägt auch das fehl, wird der Benutzer aufgefordert, das Installationsmedium einzulegen.

Wird ein Treiber gefunden, prüft das Betriebssystem, ob der Benutzer berechtigt ist, das Treiberpaket zum Treiberspeicher hinzuzufügen. Der Benutzer muss dazu Anmeldeinformationen eines Administrators haben oder die Computerrichtlinie muss so eingestellt sein, dass Standardbenutzern die Installation des identifizierten Geräts erlaubt ist. Windows 7 prüft nun, ob das Treiberpaket eine gültige digitale Signatur hat. Falls das Treiberpaket unsigniert ist oder mit einem Zertifikat signiert wurde, das nicht im Speicher der vertrauenswürdigen Herausgeber aufgelistet ist, fragt Windows 7 beim Benutzer nach, ob er den Vorgang erlaubt. Genehmigt ein autorisierter Benutzer den Treiber, legt das Betriebssystem eine Kopie des Treiberpakets in den Treiberspeicher, worauf die Installation fortgesetzt wird.

Windows führt im Rahmen des Stagings alle erforderlichen Sicherheitsprüfungen aus, darunter die Überprüfung der Administratorrechte und der digitalen Signaturen. Wurde ein Treiberpaket erfolgreich bereitgestellt, kann jeder Benutzer, der sich an diesem Computer anmeldet, die Treiber aus dem Treiberspeicher installieren, indem er einfach das entsprechende Gerät ansteckt. Dabei muss er keine Eingabeaufforderungen bestätigen und braucht auch keine speziellen Berechtigungen.

Schnelltest

- Sie haben vier Geräte an einen passiven USB-Hub angesteckt. Sie haben einen Hub mit eigener Stromversorgung, auf dem noch ein Anschluss frei ist, und denken, dass sich die Hardwareleistung verbessert, wenn Sie ein Gerät vom ersten Hub auf den zweiten umstecken. Wie stellen Sie fest, welches der Geräte auf dem passiven Hub am meisten Strom verbraucht?

Antwort zum Schnelltest

- Klicken Sie im Geräte-Manager doppelt auf *USB-Controller*. Klicken Sie mit der rechten Maustaste auf den passiven USB-Hub und wählen Sie den Befehl *Eigenschaften*. Sehen Sie sich auf der Registerkarte *Stromversorgung* in der Liste *Angeschlossene Geräte* an, wie viel jedes Gerät benötigt.



Weitere Informationen Treiberspeicher und Stagingprozess

Weitere Informationen über den Treiberspeicher und den Stagingprozess finden Sie unter *http://technet.microsoft.com/en-us/library/cc754052.aspx*. Diese Seite behandelt Windows Server 2008 und Windows Vista, die Informationen gelten aber genauso für Windows 7.

Installieren eines Nicht-PnP-Geräts

Ist ein Gerät nicht PnP-fähig (beispielsweise ein älteres Gerät), muss das angemeldete Konto über Administratorberechtigungen verfügen, um es zu installieren. Falls der Hersteller ein Installationsmedium zu seinem Gerät mitliefert, empfiehlt Microsoft, dieses Medium einzulegen und die enthaltene Installationssoftware zu benutzen. Üblicherweise erledigen Sie das, bevor Sie das Gerät anstecken.

Andernfalls müssen Sie den Geräte-Manager starten, ganz oben in der Strukturansicht mit der rechten Maustaste auf den Computernamen klicken und den Befehl *Legacyhardware hinzufügen* wählen. Daraufhin wird der Hardware-Assistent gestartet (Abbildung 4.8).

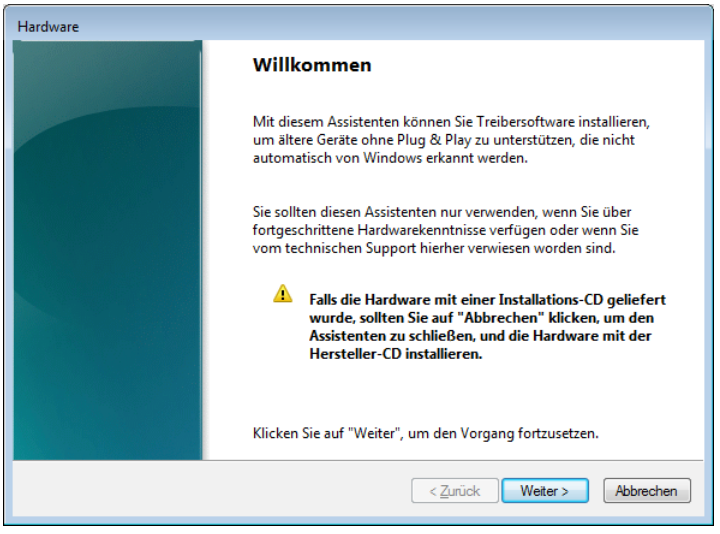

Hardware
Willkommen
Mit diesem Assistenten können Sie Treibersoftware installieren, um ältere Geräte ohne Plug & Play zu unterstützen, die nicht automatisch von Windows erkannt werden.
Sie sollten diesen Assistenten nur verwenden, wenn Sie über fortgeschrittene Hardwarekenntnisse verfügen oder wenn Sie vom technischen Support hierher verwiesen worden sind.
Falls die Hardware mit einer Installations-CD geliefert wurde, sollten Sie auf "Abbrechen" klicken, um den Assistenten zu schließen, und die Hardware mit der Hersteller-CD installieren.
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
< Zurück
Weiter >
Abbrechen

Abbildung 4.8 Der Hardware-Assistent

Der Assistent lässt Ihnen die Wahl, ob Sie ihn nach der Hardware suchen lassen oder Hardware installieren wollen, die Sie selbst aus einer Liste auswählen. Im ersten Fall muss das Gerät an den Computer angeschlossen sein. Der Ablauf ist derselbe wie beim Staging von PnP-Hardware, die nicht vorher autorisiert wurde.

Wenn Sie entscheiden, die Hardware selbst auszuwählen, bekommen Sie eine Liste der Gerätetypen angezeigt. Wählen Sie hier *Alle Geräte anzeigen* aus, bekommen Sie alle Geräte nach den Herstellern sortiert aufgelistet, sodass Sie das Gerät auswählen können (Abbildung 4.9). Wenn Sie den Treiber (es muss nicht unbedingt ein Treiberinstallationspaket sein) auf einem Wechseldatenträger oder in einem Ordner auf Ihrer Festplatte vorliegen haben, können Sie stattdessen auf *Datenträger* klicken.

Sobald Sie einen Treiber ausgewählt haben, installiert der Assistent Ihre Hardware. Falls Probleme mit der Hardware auftreten (wenn Sie etwa einen Code-10-Fehler erhalten, dass das Gerät nicht gestartet werden kann), werden sie auf der letzen Seite des Assistenten aufgelistet.

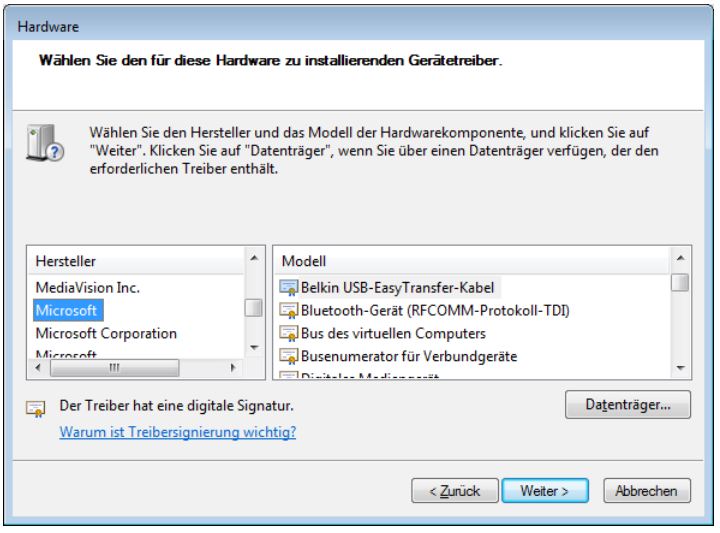

Hardware
Wählen Sie den für diese Hardware zu installierenden Gerätetreiber.
Wählen Sie den Hersteller und das Modell der Hardwarekomponente, und klicken Sie auf "Weiter". Klicken Sie auf "Datenträger", wenn Sie über einen Datenträger verfügen, der den erforderlichen Treiber enthält.
Hersteller
MediaVision Inc.
Microsoft
Microsoft Corporation
Modell
Belkin USB-EasyTransfer-Kabel
Bluetooth-Gerät (RFCOMM-Protokoll-TDI)
Bus des virtuellen Computers
Busenumerator für Verbundgeräte
Der Treiber hat eine digitale Signatur.
Warum ist Treibersignierung wichtig?
Datenträger...
< Zurück
Weiter >
Abbrechen

Abbildung 4.9 Auswählen eines Gerätetreibers

Konfigurieren von Geräteinstallationsrichtlinien

In den Übungen weiter unten in dieser Lektion stellen Sie mit dem Editor für lokale Gruppenrichtlinien fest, dass Nicht-Administratoren Geräte einer bestimmten Gerätesetupklasse installieren dürfen. Sie können mit diesem Tool auch andere Geräteinstallationsrichtlinien konfigurieren. Erweitern Sie im Editor für lokale Gruppenrichtlinien die Knoten *Computerkonfiguration*, *Administrative Vorlagen*, *System* und *Geräteinstallation*, klicken Sie auf *Einschränkungen bei der Geräteinstallation* und aktivieren Sie im rechten Fensterabschnitt die Registerkarte *Standard*. Diese Registerkarte listet die Richtlinien auf (Abbildung 4.10).

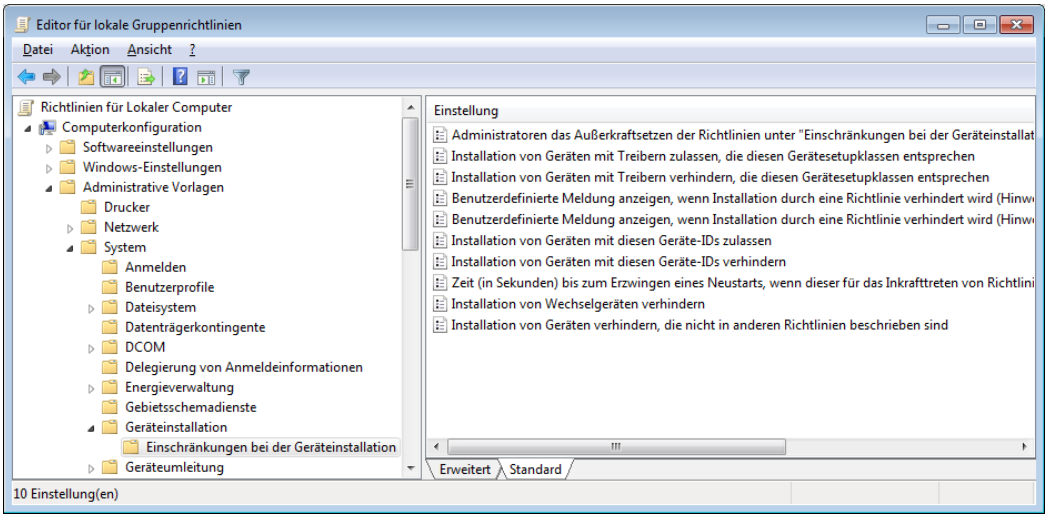

Editor für lokale Gruppenrichtlinien
Datei Aktion Ansicht ?
Richtlinien für Lokaler Computer
Computerkonfiguration
Softwareeinstellungen
Windows-Einstellungen
Administrative Vorlagen
Drucker
Netzwerk
System
Anmelden
Benutzerprofile
Dateisystem
Datenträgerkontingente
DCOM
Delegierung von Anmeldeinformationen
Energieverwaltung
Gebietsschemadienste
Geräteinstallation
Einschränkungen bei der Geräteinstallation
Geräteumleitung
Einstellung
Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallat
Installation von Geräten mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen
Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen
Benutzerdefinierte Meldung anzeigen, wenn Installation durch eine Richtlinie verhindert wird (Hinw
Benutzerdefinierte Meldung anzeigen, wenn Installation durch eine Richtlinie verhindert wird (Hinw
Installation von Geräten mit diesen Geräte-IDs zulassen
Installation von Geräten mit diesen Geräte-IDs verhindern
Zeit (in Sekunden) bis zum Erzwingen eines Neustarts, wenn dieser für das Inkrafttreten von Richtlini
Installation von Wechselgeräten verhindern
Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind
Erweitert Standard
10 Einstellung(en)

Abbildung 4.10 Richtlinien für Einschränkungen bei der Geräteinstallation

Mithilfe dieser Richtlinien können Sie folgende Einstellungen vornehmen:

- Mitgliedern der Administratorengruppe erlauben, die Treiber für alle Geräte zu installieren und zu aktualisieren, unabhängig davon, welche anderen Richtlinieneinstellungen konfiguriert sind
- Windows 7 erlauben, Gerätetreiber, deren Gerätesetupklassen-GUID (Globally Unique Identifier) Sie angeben, zu installieren oder zu aktualisieren, sofern keine andere Richtlinieneinstellung die Installation explizit verbietet
- Verhindern, dass Windows 7 Gerätetreiber, deren Gerätesetupklassen-GUID (Globally Unique Identifier) Sie angeben, installiert oder aktualisiert. Diese Richtlinie hat Vorrang vor allen anderen Richtlinien, die eine Aktualisierung oder Installation erlauben.
- Anzeigen einer angepassten Meldung für die Benutzer in der Benachrichtigungssprechblase, wenn eine Geräteinstallation versucht wird, aber eine Richtlinieneinstellung die Installation verhindert
- Anzeigen eines benutzerdefinierten Meldungstitels in der Benachrichtigungssprechblase, wenn eine Geräteinstallation versucht wird, aber eine Richtlinieneinstellung die Installation verhindert
- Angeben einer Liste von PnP-Hardware-IDs und kompatibler IDs für Geräte, die Windows installieren darf. Andere Richtlinieneinstellungen, die eine Geräteinstallation verhindern, haben Vorrang vor dieser Richtlinie.
- Angeben einer Liste von PnP-Hardware-IDs und kompatibler IDs für Geräte, die Windows nicht installieren darf. Diese Richtlinie hat Vorrang vor allen anderen Richtlinien, die eine Installation erlauben.
- Festlegen, wie lange (in Sekunden) das System bis zu einem Neustart wartet, um eine Änderung an den Richtlinien für Einschränkungen bei der Geräteinstallation zu erzwingen
- Verhindern, dass Windows 7 Wechselmediengeräte installiert. Diese Richtlinie hat Vorrang vor allen anderen Richtlinieneinstellungen, die Windows 7 die Installation eines Wechselmediengeräts erlauben.
- Verhindern, dass Geräte installiert werden, sofern sie nicht explizit durch eine andere Richtlinieneinstellung abgedeckt werden

Sie öffnen den Editor für lokale Gruppenrichtlinien, indem Sie im Suchfeld des Startmenüs **gpedit.msc** eingeben. Es wird dringend empfohlen, doppelt auf jede Richtlinie in *Einschränkungen bei der Geräteinstallation* (und im Knoten *Geräteinstallation*) zu klicken und sich die Erklärungen durchzulesen. Die Richtlinien im Editor für lokale Gruppenrichtlinien zu untersuchen, ist eine der vorgeschlagenen Übungen am Ende dieses Kapitels.

Arbeiten mit Gerätetreibern

Wie Sie bereits erfahren haben, werden beim Installieren eines Hardwaregeräts zuerst die Installationsdateien des Gerätetreibers gesucht, und dann wird der Treiber installiert. Sobald der Treiber installiert ist, können Sie ihn aktualisieren (indem Sie einen neueren Treiber installieren), deinstallieren, deaktivieren und wieder aktivieren. Falls Sie einen Treiber aktualisiert haben und nun feststellen, dass der neue Treiber nicht so gut funktioniert wie die ältere Version, können Sie die Version des Treibers wiederherstellen, die vor dem Update installiert war.

Wenn ein aktualisierter Gerätetreiber über Windows Update verteilt wird, wird er normalerweise automatisch installiert, wenn Sie dem Download zustimmen. Gewöhnlich nutzen Sie die Updatefunktion, wenn der Hersteller einen neuen oder aktualisierten Gerätetreiber veröffentlicht, bevor er in Windows Update verteilt wird. Um die neuste Version des Treibers zu erhalten und ihn auf Ihrem Windows 7-Referenzcomputer zu testen, müssen Sie die Treiberdateien von der Website des Herstellers herunterladen und den Treiber dann von Hand aktualisieren.

Wenn Sie einen Treiber aktualisieren, laufen ähnliche Operationen ab wie bei der Installation eines Treibers, sobald neue Hardware an den Computer angesteckt wird. Wenn der Treiber bereits autorisiert wurde und im Treiberspeicher vorliegt oder wenn ein Administrator ihn mithilfe von Staging bereitgestellt hat, läuft der Updateprozess, wenn er erst einmal gestartet wurde, automatisch ohne Benutzereingaben ab. Andernfalls können Sie Windows 7 erlauben, nach Treibern für das Hardwaregerät zu suchen, oder von Hand eine Ordneradresse angeben, wie im Abschnitt »Installieren eines Nicht-PnP-Geräts« weiter oben in dieser Lektion beschrieben. Wird ein Treiber gefunden, der neuer ist als der bereits installierte, wird der Administrator aufgefordert, ihn zu genehmigen.

Sie haben zwei Möglichkeiten, den Prozess zur Treiberaktualisierung im Geräte-Manager zu starten:

- Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie den Befehl *Treibersoftware aktualisieren*.
- Klicken Sie doppelt auf das Gerät. Klicken Sie auf der Registerkarte *Treiber* auf *Treiber aktualisieren*.

Sie können entweder einen neuen Treiber installieren oder einen, der aktualisiert wurde. Stellen Sie allerdings fest, dass die aktuelle Treiberinstallation beschädigt ist, wird der aktuelle Treiber nicht erneut installiert, nur weil Sie ihn aktualisieren. In diesem Fall müssen Sie den Treiber deinstallieren und anschließend neu installieren. Wie beim Aktualisieren eines Treibers können Sie entweder im Geräte-Manager mit der rechten Maustaste auf das Gerät klicken und den Befehl *Deinstallieren* wählen oder doppelt auf das Gerät klicken und dann auf der Registerkarte *Treiber* auf die Schaltfläche *Deinstallieren* klicken. Abbildung 4.11 zeigt die Registerkarte *Treiber*.

Gelegentlich lassen sich Probleme beseitigen, indem Sie das Gerät deaktivieren, statt einen Treiber zu deinstallieren und dann neu zu installieren. Falls ein Treiberkonflikt aufgetreten ist, müssen Sie wahrscheinlich einen der Treiber deaktivieren oder beenden, sofern es sich um ein Nicht-PnP-Gerät handelt.

Sie können die Vorversion eines Treibers nicht wiederherstellen, indem Sie das Gerät im Geräte-Manager mit der rechten Maustaste anklicken. Dazu müssen Sie die Registerkarte *Treiber* des Geräts öffnen. Sofern der Treiber noch nie aktualisiert wurde, ist die Schaltfläche *Vorheriger Treiber* deaktiviert. Im Allgemeinen stellen Sie die Vorversion eines Treibers wieder her, wenn Sie einen Gerätetreiber aktualisiert haben, aber der neue Treiber nicht so gut funktioniert wie der ältere oder Konflikte mit anderen Treibern verursacht. In diesem Fall müsste der ältere Treiber noch im Treiberspeicher vorhanden sein, sodass der Prozess ohne Benutzereingaben abläuft (unter Umständen müssen Sie die Operation mit einem Klick auf *Ja* erlauben).

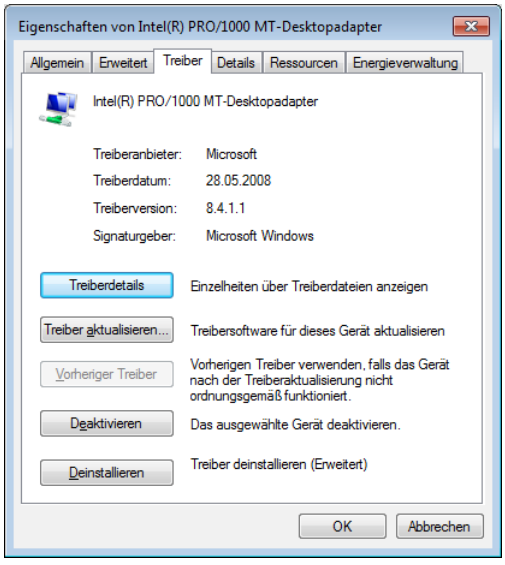


Abbildung 4.11 Die Registerkarte *Treiber*

Wenn Sie Probleme im Zusammenhang mit einem Treiber untersuchen oder aus einem anderen Grund mehr darüber herausfinden wollen, können Sie auf der Registerkarte *Treiber* auf *Treiberdetails* klicken. Abbildung 4.12 zeigt die Treiberdetails zu einem Netzwerkadaptertreiber.

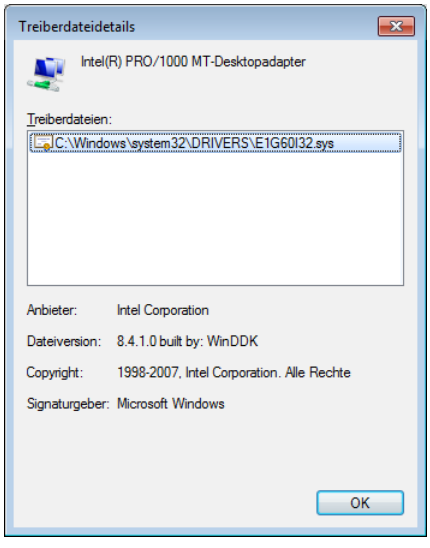


Abbildung 4.12 Treiberdetails

Die Treiberdetails geben unter anderem an, wo die verwendete Treiberdatei gespeichert ist. Beachten Sie, dass dies nicht der Treiberspeicher ist, der sich in einem geschützten Bereich befindet. Außerdem erfahren Sie hier Dateinamen und -typ. Laufende Treiberdateien arbeiten so, als wären sie ein Teil des Betriebssystems. Meist haben Sie die Erweiterung *.sys*. Treiber-

installationsdateien haben die Erweiterung *.inf*. Die Treiberdetails führen den Anbieter (normalerweise ein Hardwarehersteller), die Dateiversion, den Signaturgeber (meist Microsoft) und Copyrightinformationen auf. Oft ist es nützlich, die Dateiversion zu wissen, wenn Probleme mit einem Treiber auftreten und Sie im Internet nach Informationen suchen, etwa in Microsoft-Blogs. Vielleicht finden Sie eine Meldung in der Art »Version 10.0.5.3 hat dieses Problem. Deinstallieren Sie sie und installieren Sie stattdessen Version 10.0.5.2.«

Beseitigen von Treiberkonflikten

Treiberkonflikte sind heutzutage viel seltener als früher. Vor 15 Jahren war es nicht weiter ungewöhnlich, dass die Maus ausfiel, wenn man einen Drucker anschloss. Fast die gesamte moderne Hardware ist PnP-fähig. Das Betriebssystem steuert die Installation, weshalb Konflikte normalerweise vermieden werden. Allerdings ist kein System perfekt. Es ist nach wie vor möglich, dass ein Konflikt auftritt.

In den meisten Fällen tritt ein Konflikt auf, wenn zwei Geräte dieselben Ressourcen brauchen, vor allem wenn sich ihre Interrupt- oder E/A-Anforderungen überschneiden. Sie können die Ressourcennutzung auf der Registerkarte *Ressourcen* im Eigenschaftendialogfeld eines Geräts ermitteln (Abbildung 4.13). Bei den meisten Gerätetreibern ist *Automatisch konfigurieren* ausgewählt, und *Einstellung ändern* ist deaktiviert.

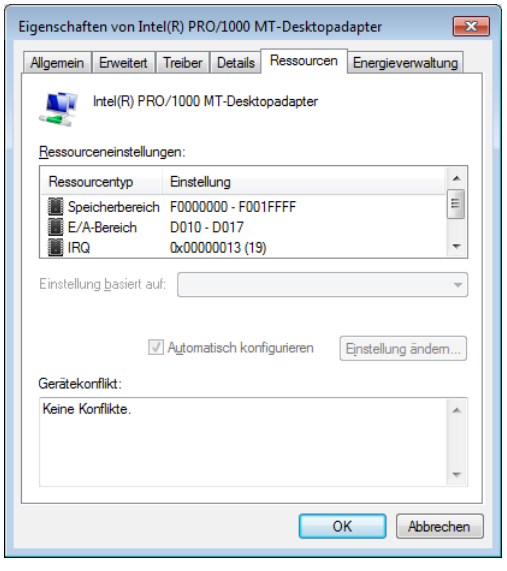


Abbildung 4.13 Die Registerkarte *Ressourcen*

Konflikte zwischen PnP-Geräten sind ungewöhnlich. Sie lassen sich kurzfristig beseitigen, indem Sie eines der Geräte deaktivieren. Wenn Sie den Treiber aktualisieren (sofern ein Update verfügbar ist) oder die Hardware deinstallieren und wieder neu installieren, ist der Konflikt wahrscheinlich beseitigt.

Abbildung 4.14 zeigt eine Konfliktsituation, bei der ein Nicht-PnP-Gerät Ressourcen benutzt, die auch vom Motherboard gebraucht werden. Ist ein Nicht-PnP-Gerät an einem Konflikt beteiligt, müssen Sie dieses Gerät unter Umständen beenden, um das Problem zu beseitigen.

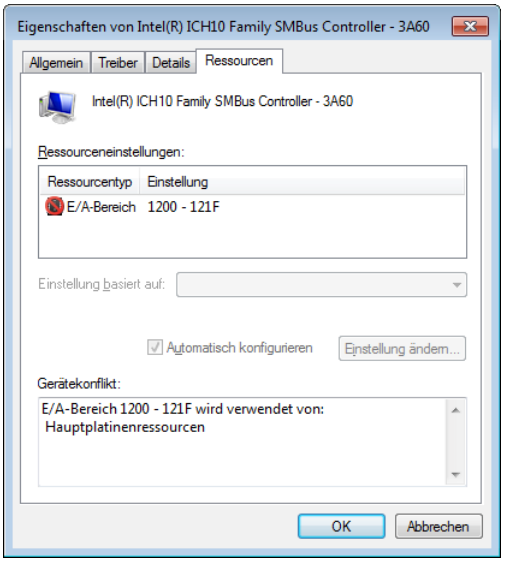


Abbildung 4.14 Ein Ressourcenkonflikt

Gehen Sie folgendermaßen vor, um ein Nicht-PnP-Gerät zu beenden:

1. Öffnen Sie den Geräte-Manager.
2. Wählen Sie im Menü *Ansicht* den Befehl *Ausgeblendete Geräte anzeigen*.
3. Klicken Sie doppelt auf *Nicht-PnP-Treiber*, klicken Sie mit der rechten Maustaste auf das Gerät, das Sie beenden wollen, und wählen Sie den Befehl *Eigenschaften*.
4. Klicken Sie auf der Registerkarte *Treiber* (Abbildung 4.15) auf *Beenden* und dann auf *OK*.

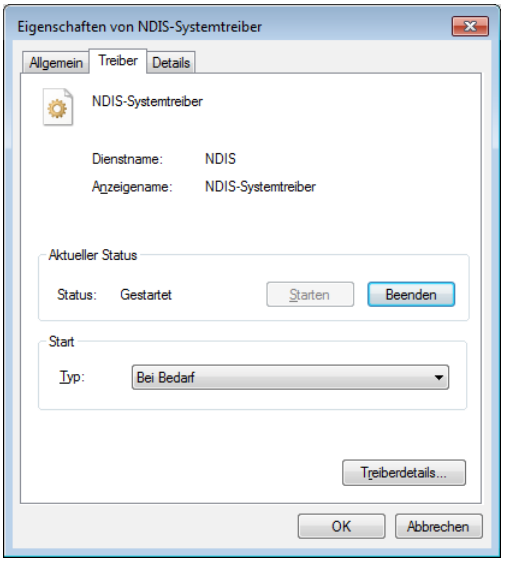


Abbildung 4.15 Die Registerkarte *Treiber* bei einem Nicht-PnP-Gerät

Wollen Sie ein Gerät neu starten, gehen Sie praktisch genauso vor, allerdings klicken Sie in diesem Fall auf *Starten* statt auf *Beenden*. Sie können auf dieser Registerkarte auch den Starttyp ändern. Falls die Schaltfläche *Starten* auf der Registerkarte *Treiber* deaktiviert ist, wurde der Treiber bereits geladen.

Ermitteln von Ressourcenkonflikten mit dem Tool *Systeminformationen*

Wenn Sie vermuten, dass ein Gerätetreiber aufgrund von Ressourcenkonflikten nicht richtig funktioniert, können Sie sich die E/A- und IRQ-Anforderungen aller Geräte mit dem Tool *Systeminformationen* (Msinfo32) ansehen. Dafür ein einziges Tool zu verwenden, ist bequemer, als bei jedem einzelnen Gerät die Registerkarte *Ressourcen* zu öffnen. Sie starten Msinfo32, indem Sie im Suchfeld des Startmenüs, im Dialogfeld *Ausführen* oder in einer Eingabeaufforderung **msinfo32** eingeben. Sie brauchen keine Eingabeaufforderung mit erhöhten Rechten, um Msinfo32 zu verwenden. Das Tool liefert allgemeine Systeminformationen (Abbildung 4.16).

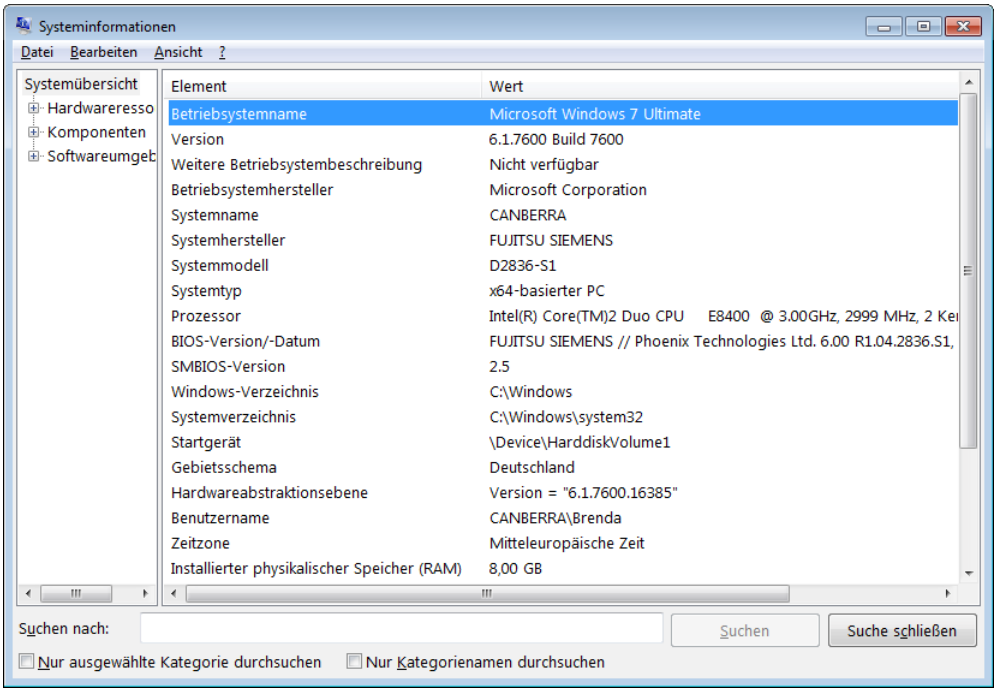


Abbildung 4.16 MSinfo32 zeigt allgemeine Systeminformationen an

Wenn Sie den Zweig *Hardwareressourcen* aufklappen, werden die Arbeitsspeicher-, E/A- und IRQ-Ressourcen aller Geräte auf dem Computer aufgelistet. Wenn Sie Konflikte beseitigen müssen, erhalten Sie die nützlichsten Informationen wahrscheinlich, indem Sie den Knoten *Konflikte/Gemeinsame Nutzung* auswählen (Abbildung 4.17). Treten Probleme bei einem bestimmten Gerät auf, können Sie danach suchen, indem Sie seinen Namen im Textfeld *Suchen nach* eingeben. So erfahren Sie, welche Geräte dieselben Ressourcen nutzen, und können mögliche Konflikte analysieren.

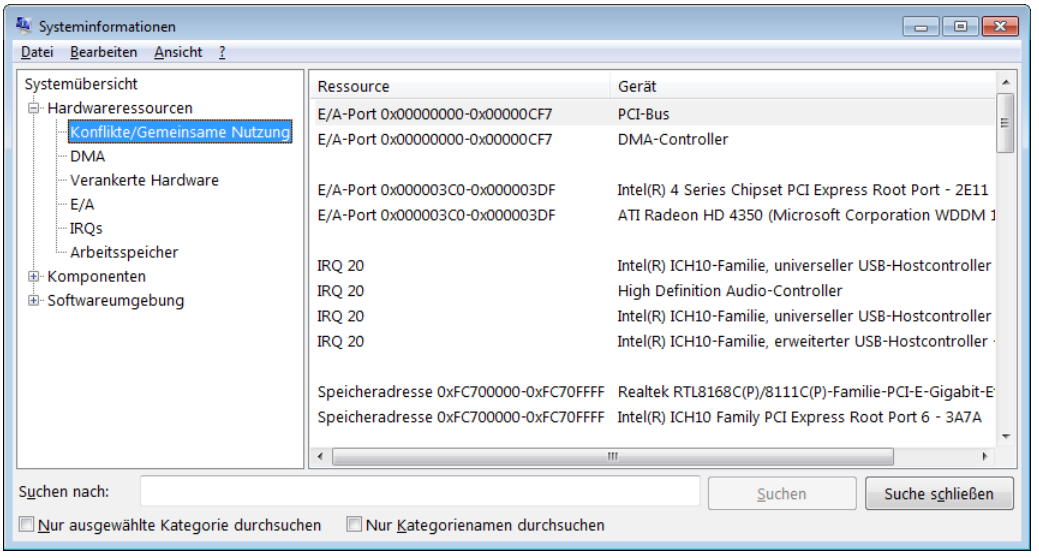


Abbildung 4.17 MSinfo32 liefert Informationen über Konflikte und gemeinsam genutzte Ressourcen

Informationen über bestimmte Geräte (CD, Audiogerät, Anzeige und so weiter) erhalten Sie, wenn Sie die entsprechenden Knoten unter *Komponenten* auswählen. Am nützlichsten für Diagnosezwecke ist die Rubrik *Problemgeräte*, wo Geräte aufgelistet sind, die nicht gestartet werden konnten, für die keine Treiber installiert sind oder bei denen andere Probleme aufgetreten sind.

Wenn Sie den Knoten *Softwareumgebung* aufklappen, steht der Knoten *Systemtreiber* zur Verfügung. Er zeigt eine Liste der Kerneltreiber an, in der Sie feststellen können, ob ein Treiber gestartet wurde. Wenn Sie einen bestimmten Treiber suchen, können Sie seinen Dateinamen oder die Beschreibung in das Textfeld *Suchen nach* eingeben.

Testen von Treibern mit dem Treiberüberprüfungs-Manager

Nicht alle Treiberprobleme werden durch Konflikte verursacht. Manchmal sind Geräte einfach defekt oder es treten Abbruchfehler auf, obwohl keine Informationen über Konflikte angezeigt werden und sich die Probleme durch Deaktivieren anderer Treiber nicht beseitigen lassen. Wie bei jeder Softwareinstallation können Sie mithilfe der Zuverlässigkeitsüberwachung feststellen, wann die Installation durchgeführt wurde und ob die Zuverlässigkeit darunter gelitten hat. Aber dieses Tool ist nicht in der Lage, konkrete Gerätetreiberprobleme zu diagnostizieren.

Windows 7 stellt das Befehlszeilentool Treiberüberprüfungs-Manager (driver verifier monitor) zur Verfügung, mit dem Sie Gerätetreiber überwachen können, um unerlaubte Funktionsaufrufe oder Aktionen aufzuspüren, die das System unter Umständen beschädigen. Es kann die Treiber verschiedenen Stresstests unterziehen, um falsches Verhalten aufzudecken.

Abbildung 4.18 zeigt den Treiberüberprüfungs-Manager, der mit dem Befehl `verifier` gestartet wird. Mit dem Flag `/volatile` können Sie die Überprüfung eines Treibers starten, ohne den Computer neu zu starten; das funktioniert sogar dann, wenn der Treiberüberprüfungs-Manager noch nicht läuft. Außerdem können Sie die Überprüfung eines Treibers

starten, der bereits geladen ist. Dank dieser Verbesserungen, die schon in Windows Vista eingeführt wurden, müssen Sie das System nicht mehr so oft neu starten. Das spart Zeit, und Sie können mit dem Treiberüberprüfungs-Manager einen Treiber überwachen, während Sie Geräte anschließen und wieder entfernen.

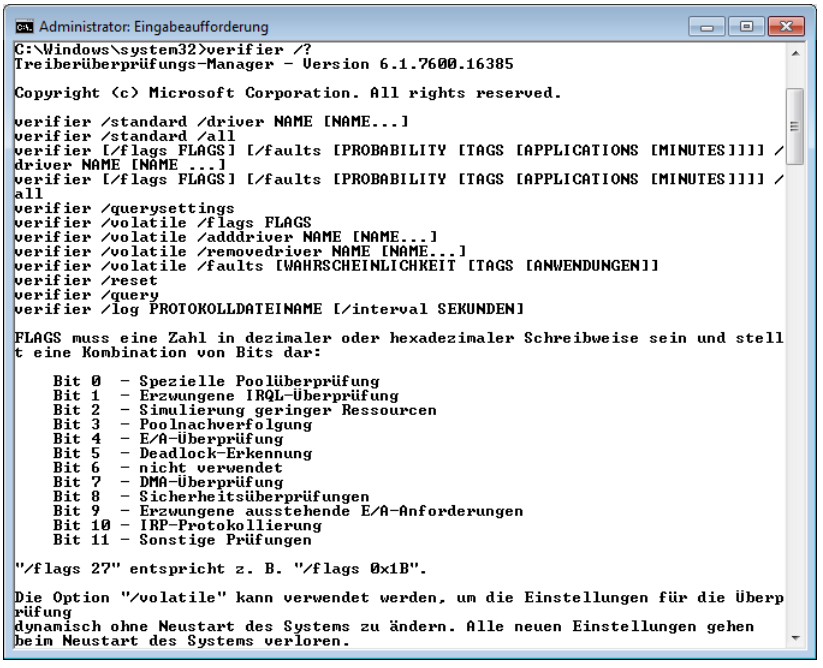

Administrator: Eingabeaufforderung
C:\Windows\system32>verifier /?
Treiberüberprüfungs-Manager - Version 6.1.7600.16385
Copyright (c) Microsoft Corporation. All rights reserved.
verifier /standard /driver NAME [NAME...]
verifier /standard /all
verifier [/flags FLAGS] [/faults [PROBABILITY [TAGS [APPLICATIONS [MINUTES]]]] /
driver NAME [NAME ...]
verifier [/flags FLAGS] [/faults [PROBABILITY [TAGS [APPLICATIONS [MINUTES]]]] /
all
verifier /querysettings
verifier /volatile /flags FLAGS
verifier /volatile /adddriver NAME [NAME...]
verifier /volatile /removedriver NAME [NAME...]
verifier /volatile /faults [WAHRSCHEINLICHKEIT [TAGS [ANWENDUNGEN]]]
verifier /reset
verifier /query
verifier /log PROTOKOLLDATEINAME [/interval SEKUNDEN]
FLAGS muss eine Zahl in dezimaler oder hexadezimaler Schreibweise sein und stell
t eine Kombination von Bits dar:
Bit 0 - Spezielle Poolüberprüfung
Bit 1 - Erzwungene IRQL-Überprüfung
Bit 2 - Simulierung geringer Ressourcen
Bit 3 - Poolnachverfolgung
Bit 4 - E/A-Überprüfung
Bit 5 - Deadlock-Erkennung
Bit 6 - nicht verwendet
Bit 7 - DMA-Überprüfung
Bit 8 - Sicherheitsüberprüfungen
Bit 9 - Erzwungene ausstehende E/A-Anforderungen
Bit 10 - IRP-Protokollierung
Bit 11 - Sonstige Prüfungen
"/flags 27" entspricht z. B. "/flags 0x1B".
Die Option "/volatile" kann verwendet werden, um die Einstellungen für die Überp
rüfung
dynamisch ohne Neustart des Systems zu ändern. Alle neuen Einstellungen gehen
beim Neustart des Systems verloren.

Abbildung 4.18 Der Treiberüberprüfungs-Manager

Sie können Einstellungen abfragen und Treiber hinzufügen oder entfernen, aber die wichtigste Funktion erreichen Sie über das Flag `/faults`. Damit lösen Sie Stresstests mit einstellbarem Schweregrad aus, um festzustellen, ob der Treiber in allen Situationen richtig funktioniert. Sie können beispielsweise den Fall simulieren, dass die Ressourcen knapp werden, oder den Fall, dass eine längere Wartezeit auftritt, nach der ein unerwartetes Ergebnis zurückgegeben wird. Sie können die Ressourcennutzung (Poolzuweisung) überwachen und aufzeichnen, wie viele Fehler in ein System eingespeist werden.

Der Treiberüberprüfungs-Manager ist in erster Linie ein Tool für Stresstests. Es informiert Sie beispielsweise darüber, dass ein Gerätetreiber ausfällt, wenn Datenträger- oder Arbeitsspeicherauslastung eine bestimmte Grenze überschreiten. Sie können Tools mit allgemeinerer Zielsetzung wie Systemmonitor und Task-Manager einsetzen, um die Ressourcennutzung zu überwachen und Situationen zu diagnostizieren, in denen die Ressourcen knapp werden.



Weitere Informationen Treiberüberprüfungs-Manager

Weitere Informationen über den Treiberüberprüfungs-Manager finden Sie im Whitepaper »Driver Verifier in Windows Vista«, das Sie unter *http://www.microsoft.com/whdc/devtools/tools/vistaverifier.mspx* herunterladen können. Dieses Dokument beschreibt die Verwendung des Tools in Windows Vista, die Informationen gelten aber genauso für Windows 7.

Treibersignierung und digitale Zertifikate

Digitale Signaturen erlauben es Administratoren und Benutzern, die Windows-Software installieren, festzustellen, ob das Softwarepaket von einem bekannten Herausgeber stammt. Es werden Administratorprivilegien gebraucht, um unsignierte Kernelmodusfeatures wie Gerätetreiber zu installieren. Treiber müssen mit Zertifikaten signiert sein, denen Windows 7 vertraut. Zertifikate, die vertrauenswürdige Zertifizierungsstellen identifizieren, sind im Zertifikatspeicher *Vertrauenswürdige Herausgeber* gespeichert.

Als Administrator können Sie die Installation eines Treibers autorisieren, der unsigniert ist oder dessen Herausgeber nicht im Speicher *Vertrauenswürdige Herausgeber* aufgelistet ist. Wenn Sie den Treiber nicht im ganzen Unternehmen verteilen, sondern ihn lediglich auf einem Testcomputer installieren, um ihn auszuprobieren, gibt es daran nichts auszusetzen. Viele Treiber stammen aus unverdächtigen Quellen (etwa vom Gerätehersteller), haben aber noch nicht den gesamten Überprüfungsprozess durchlaufen, der Voraussetzung für eine digitale Signatur ist. Selbst einige Microsoft-Treiber sind unsigniert.

Wenn Sie oder andere Administratoren Treiber installieren, ist die Autorisierung normalerweise kein Problem. Anders sieht es aus, wenn Sie einen Treiber haben, den auch normale Benutzer installieren sollen. Selbst wenn Sie den Treiber durch Staging bereitstellen, können die Benutzer ihn nicht installieren, weil nur Administratoren die Installation eines Treibers ohne gültige Signatur genehmigen dürfen.

Sie können sich ein selbstsigniertes Zertifikat besorgen, das innerhalb Ihrer Organisation gilt. Dafür brauchen Sie einen Zertifizierungsstellenserver, der unter einem Windows Server-Betriebssystem läuft und die Zertifikatdienste ausführt. Andere Organisationen, zu denen keine Vertrauensstellung besteht, vertrauen diesem Zertifikat nicht. Microsoft empfiehlt, dass Sie diese Methode sogar innerhalb Ihrer eigenen Organisation nur in einem Testnetzwerk verwenden. In der Produktivumgebung sollten Sie ausschließlich Treiber installieren, die eine gültige Signatur haben.

Wenn Sie einen Gerätetreiber so signieren wollen, dass er auch von anderen Organisationen benutzt werden kann, brauchen Sie ein Zertifikat, das von einer vertrauenswürdigen externen Zertifizierungsstelle wie VeriSign ausgestellt wurde. Ein solches Zertifikat ist wesentlich schwieriger zu bekommen.

Damit auch Nicht-Administratoren einen Treiber installieren können, der keine vertrauenswürdige Signatur hat, müssen Sie das Gerätetreiberpaket mit einem digitalen Zertifikat signieren und dieses Zertifikat dann auf den Clientcomputern speichern, sodass die Benutzer nicht erst feststellen müssen, ob ein Gerätetreiber oder sein Herausgeber »vertrauenswürdig« ist.

Anschließend stellen Sie das Gerätetreiberpaket im geschützten Treiberspeicher eines Clientcomputers bereit (wie weiter oben in dieser Lektion beschrieben), damit ein Standardbenutzer das Paket installieren kann, ohne Administratorprivilegien zu benötigen.

Normalerweise verwenden Sie Gruppenrichtlinien, um das Zertifikat auf den Clientcomputern bereitzustellen. Mithilfe von Gruppenrichtlinien können Sie das Zertifikat automatisch auf allen verwalteten Computern in einer Domäne, einer Organisationseinheit oder einem Standort installieren.

Eine digitale Signatur garantiert, dass ein Paket tatsächlich von der angegebenen Quelle stammt (Authentizität), garantiert unbeschädigt ist und nicht manipuliert wurde (Integrität).

Ein digitales Zertifikat identifiziert eine Organisation. Es ist vertrauenswürdig, weil es von einer Zertifizierungsstelle elektronisch überprüft werden kann.

Sie gehen folgendermaßen vor, um einen Gerätetreiber zu signieren:

1. Erstellen Sie ein digitales Zertifikat für die Signatur. Das erledigen Sie in der Konsole *Zertifikate* des Zertifikatservers (der Zertifizierungsstelle). Sie können auch das Tool MakeCert verwenden.
2. Fügen Sie das Zertifikat zum Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* hinzu. Diese Kopieroperation können Sie mithilfe der Zwischenablage in der Konsole *Zertifikate* ausführen, in der Sie auf den Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* Zugriff haben.
3. Fügen Sie das Zertifikat zum Zertifikatspeicher *Vertrauenswürdige Herausgeber* hinzu. Auch dafür können Sie die Konsole *Zertifikate* verwenden.
4. Signieren Sie das Gerätetreiberpaket mit dem Zertifikat. Bereiten Sie dazu die *.inf*-Datei des Treiberpakets vor, legen Sie eine Katalogdatei für das Treiberpaket an und signieren Sie die Katalogdatei mit dem Programm Signtool.



Prüfungstipp

Der Prozess, um einen Gerätetreiber digital zu signieren, wurde absichtlich recht allgemein beschrieben. Normalerweise erledigen Sie das auf der Ebene von Domäne, Organisationseinheit oder Standort. Es ist äußerst unwahrscheinlich, dass Sie in der Prüfung Einzelheiten zu diesem Vorgang wissen müssen. Es reicht, wenn Sie wissen, dass es möglich ist und welche Gründe es dafür gibt.



Hinweis Erzwingen der Treibersignatur deaktivieren

Wenn Sie neue Treiber, die von Ihrer Organisation entwickelt werden, testen wollen, ohne diese Treiber jedes Mal signieren zu müssen, nachdem sie aktualisiert wurden, können Sie Ihren Computer neu starten, während des Startvorgangs F8 drücken und den Menüpunkt *Erzwingen der Treibersignatur deaktivieren* auswählen. Danach dürfen Sie unsignierte Treiber verwenden, bis Sie den Computer das nächste Mal neu starten. Diese Lösung ist besonders bei den 64-Bit-Versionen von Windows 7 nützlich, wo unsignierte Treiber in der Standardeinstellung überhaupt nicht installiert werden dürfen, selbst wenn Sie Administratoranmeldeinformationen eingeben.



Weitere Informationen Erzwingen der Treibersignatur deaktivieren

Weitere Informationen über die Einstellung *Erzwingen der Treibersignatur deaktivieren* finden Sie unter *http://msdn.microsoft.com/en-us/library/aa906338.aspx*.

Prüfen von digitalen Signaturen mit dem DirectX-Diagnoseprogramm

Das DirectX-Diagnosetool (DXdiag) verwenden Sie, um Probleme im Bereich von DirectX zu analysieren. Bei manchen Problemen ist es sinnvoll zu überprüfen, ob ein Gerätetreiber für ein DirectX-Gerät (etwa Ihre Grafikkartentreiber) die Tests der Microsoft Windows Hardware Quality Labs (WHQL) durchlaufen hat und digital signiert wurde. Sie starten das Tool DXdiag, indem Sie im Suchfeld des Startmenüs, im Dialogfeld *Ausführen* oder in einer

Eingabeaufforderung **dxdiag** eingeben. Sie brauchen keine Eingabeaufforderung mit erhöhten Rechten zu öffnen, um DXdiag auszuführen.

Nach dem Start zeigt DXdiag die Registerkarte *System* an. Hier finden Sie Systeminformationen, unter anderem, welche Version von DirectX auf dem Computer installiert ist. Wenn Sie das Tool zum ersten Mal starten, sollten Sie das Kontrollkästchen *Auf digitale WHQL-Signaturen überprüfen* aktivieren (Abbildung 4.19). Diese Option bleibt ausgewählt, auch wenn Sie das Tool schließen und neu starten. Daher prüft das Tool jedes Mal, wenn Sie es ausführen, ob die Treiber digital signiert sind.

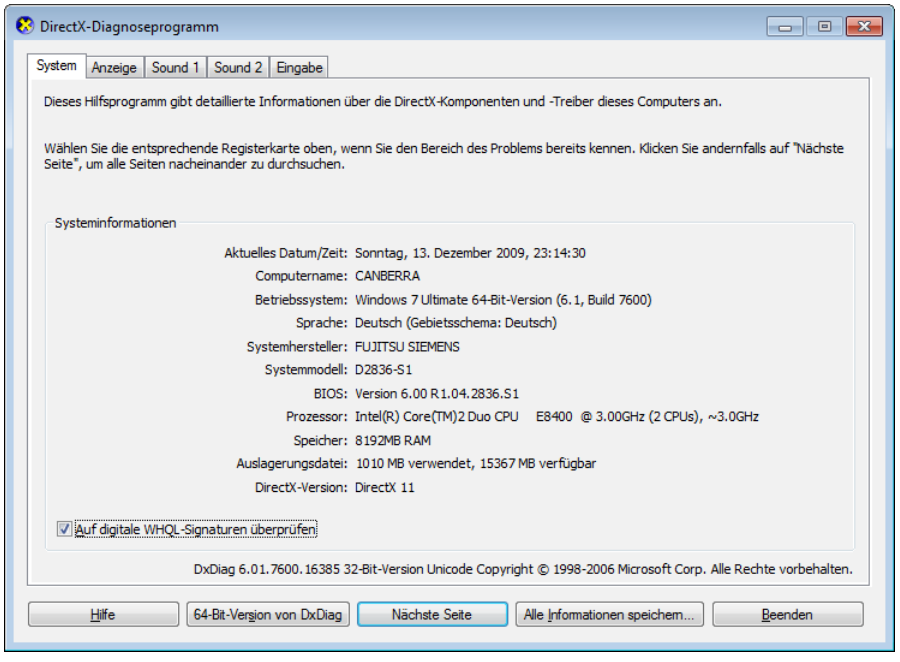

DirectX-Diagnoseprogramm
System
Anzeige
Sound 1
Sound 2
Eingabe
Dieses Hilfsprogramm gibt detaillierte Informationen über die DirectX-Komponenten und -Treiber dieses Computers an.
Wählen Sie die entsprechende Registerkarte oben, wenn Sie den Bereich des Problems bereits kennen. Klicken Sie andernfalls auf "Nächste Seite", um alle Seiten nacheinander zu durchsuchen.
Systeminformationen
Aktuelles Datum/Zeit: Sonntag, 13. Dezember 2009, 23:14:30
Computername: CANBERRA
Betriebssystem: Windows 7 Ultimate 64-Bit-Version (6.1, Build 7600)
Sprache: Deutsch (Gebietsschema: Deutsch)
Systemhersteller: FUJITSU SIEMENS
Systemmodell: D2836-S1
BIOS: Version 6.00 R1.04.2836.S1
Prozessor: Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz (2 CPUs), ~3.0GHz
Speicher: 8192MB RAM
Auslagerungsdatei: 1010 MB verwendet, 15367 MB verfügbar
DirectX-Version: DirectX 11
Auf digitale WHQL-Signaturen überprüfen
DxDiag 6.01.7600.16385 32-Bit-Version Unicode Copyright © 1998-2006 Microsoft Corp. Alle Rechte vorbehalten.
Hilfe
64-Bit-Version von DxDiag
Nächste Seite
Alle Informationen speichern...
Beenden

Abbildung 4.19 Aktivieren der Überprüfung von digitalen Signaturen im Tool DXdiag

Die Registerkarte *Anzeige* enthält Details über Ihre Anzeigehardware und -treiber. Dort ist auch der verfügbare Arbeitsspeicher für Ihre Grafikkartenhardware aufgeführt, und Sie erfahren, ob Ihr Grafikkartentreiber die WHQL-Tests durchlaufen hat. Wie in Abbildung 4.20 gezeigt, ist unter *Mit WHQL-Logo* angegeben, ob die Treiber die Tests bestanden haben.



Hinweis **Ihre Hardware hat unter Umständen mehr Grafikspeicher, als angegeben wird**

DXdiag ist nicht in der Lage, Grafikspeicher zu analysieren, der benutzt wird, während das Tool startet. Daher wird unter Umständen weniger Grafikspeicher gemeldet, als Ihre Grafikkarte tatsächlich hat.

Falls DXdiag ein Problem mit Ihren Anzeigeeinstellungen erkennt, wird eine Warnmeldung im Feld *Hinweise* ausgegeben. Andernfalls steht in diesem Feld der Text *Es wurden keine Probleme gefunden*.

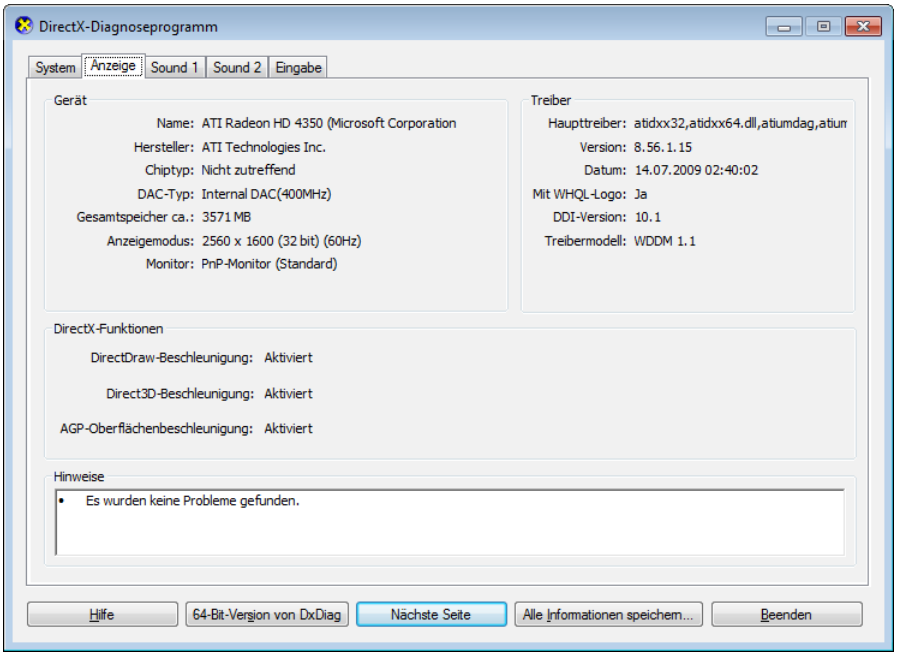


Abbildung 4.20 Die Registerkarte *Anzeige* in DXdiag

Die Registerkarte *Sound* zeigt Details über Ihre Soundhardware und -gerätetreiber an und meldet eventuelle Probleme im Feld *Hinweise*. Außerdem wird angegeben, ob der Treiber das WHQL-Logo erhalten hat. Wenn Sie mehrere Soundkarten installiert haben, werden auch mehrere *Sound*-Registerkarten angezeigt. Unter *Standardgerät* ist auf jeder dieser Registerkarten angegeben, ob das beschriebene Gerät das Standardgerät ist.

Die Registerkarte *Eingabe* listet die Eingabegeräte auf, die an Ihren Computer angeschlossen sind, sowie alle ähnlichen Geräte, die in USB-Geräte und PS/2-Geräte untergliedert sind. Sie meldet, ob Probleme mit diesen Geräten aufgetreten sind, listet aber nicht die Gerätetreiber auf und verrät auch nicht, ob sie signiert sind. Diese Informationen zu den Geräten erhalten Sie bei Bedarf im Geräte-Manager.

Überprüfen von digitalen Signaturen mit dem Tool *Dateisignaturverifizierung*

Das Tool DXdiag identifiziert Probleme mit DirectX-Hardware und verrät Ihnen, ob die Hardware die WHQL-Tests durchlaufen hat und digital signiert wurde. Es testet allerdings keine Gerätetreiber, die nichts mit DirectX-Geräten zu tun haben. Um Ihren Computer zu untersuchen und alle unsignierten Treiber zu finden, sollten Sie das Tool *Dateisignaturverifizierung* (Sigverif) verwenden.

Sie starten das Tool Sigverif, indem Sie im Suchfeld des Startmenüs, im Dialogfeld *Ausführen* oder in einer Eingabeaufforderung **sigverif** eingeben. Sie brauchen keine Eingabeaufforderung mit erhöhten Rechten, um Sigverif auszuführen. Abbildung 4.21 zeigt das Tool Sigverif.

Sie starten die Überprüfung, indem Sie auf die Schaltfläche *Starten* klicken. Wenn Sie auf *Erweitert* klicken, können Sie vor einer Überprüfung die Protokollierung konfigurieren oder sich nach Abschluss des Vorgangs die Protokolldatei ansehen. Abbildung 4.22 zeigt das

Protokoll von Sigverif. Selbst wenn Sigverif keine unsignierten Gerätetreiber findet, ist es praktisch, um alle Gerätetreiber in Ihrem Computer aufzulisten.

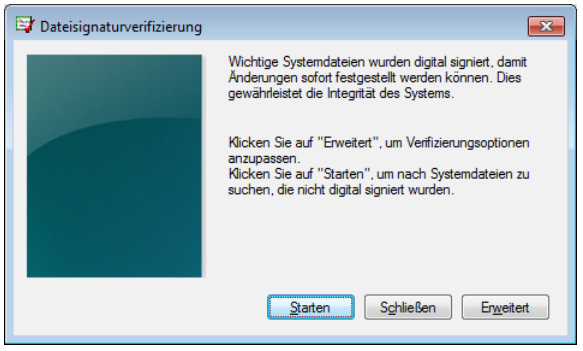

Dateisignaturverifizierung
Wichtige Systemdateien wurden digital signiert, damit Änderungen sofort festgestellt werden können. Dies gewährleistet die Integrität des Systems.
Klicken Sie auf "Erweitert", um Verifizierungsoptionen anzupassen.
Klicken Sie auf "Starten", um nach Systemdateien zu suchen, die nicht digital signiert wurden.
Starten
Schließen
Erweitert

Abbildung 4.21 Das Tool Sigverif

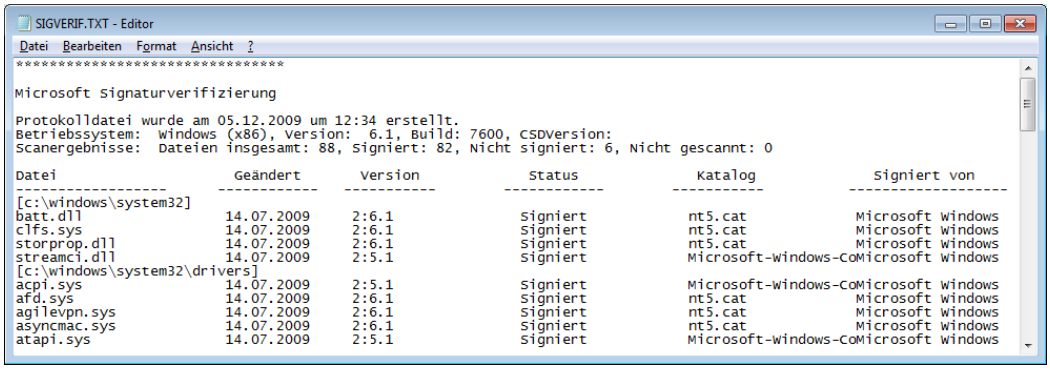

SIGVERIF.TXT - Editor
Datei Bearbeiten Format Ansicht ?
****
Microsoft Signaturverifizierung
Protokolldatei wurde am 05.12.2009 um 12:34 erstellt.
Betriebssystem: Windows (x86), Version: 6.1, Build: 7600, CSDVersion:
Scanergebnisse: Dateien insgesamt: 88, Signiert: 82, Nicht signiert: 6, Nicht gescannt: 0
Datei Geändert Version Status Katalog Signiert von
[c:\windows\system32]
batt.dll 14.07.2009 2:6.1 Signiert nt5.cat Microsoft Windows
clfs.sys 14.07.2009 2:6.1 Signiert nt5.cat Microsoft Windows
storprop.dll 14.07.2009 2:6.1 Signiert nt5.cat Microsoft Windows
streamci.dll 14.07.2009 2:5.1 Signiert Microsoft-Windows-Co Microsoft Windows
[c:\windows\system32\drivers]
acpi.sys 14.07.2009 2:5.1 Signiert Microsoft-Windows-Co Microsoft Windows
afd.sys 14.07.2009 2:6.1 Signiert nt5.cat Microsoft Windows
agilevpn.sys 14.07.2009 2:6.1 Signiert nt5.cat Microsoft Windows
asyncmac.sys 14.07.2009 2:6.1 Signiert nt5.cat Microsoft Windows
atapi.sys 14.07.2009 2:5.1 Signiert Microsoft-Windows-Co Microsoft Windows

Abbildung 4.22 Das Protokoll von Sigverif

Übung Konfigurieren von Computerrichtlinien und Treibersuche

In der Standardeinstellung dürfen nur lokale Administratoren Geräte auf einem Computer installieren. Einzige Ausnahme sind Geräte, die autorisiert wurden und deren Treiber in den Treiberspeicher gelegt wurden. Sie können die Computerrichtlinie auf einem Windows 7-Computer aber auch so konfigurieren, dass normale Benutzer Geräte installieren dürfen, solange sie zu bestimmten Gerätesetupklassen gehören. Sie haben auch die Möglichkeit, solchen Benutzern zu erlauben, Treiber auf dem Computer bereitzustellen.

Diese Anleitungen eignen sich, wenn Sie nur wenige Clientcomputer in einer Arbeitsgruppe haben. In einer Unternehmensumgebung ist es sinnvoller, die Konfiguration im Gruppenrichtlinien-Editor auf einem Domänencontroller vorzunehmen und sie dann auf die Clientcomputer anzuwenden. Dabei gehen Sie allerdings ähnlich vor wie hier beschrieben.

Außerdem konfigurieren Sie einen Windows 7-Computer so, dass er andere Verzeichnisse nach Treibern durchsucht, die sich nicht im Treiberspeicher befinden.

Übung 1 Computerrichtlinien so konfigurieren, dass Nicht-Administratoren ausgewählte Gerätesetupklassen installieren dürfen

Diese Übung erlaubt einem Standardbenutzer (Nicht-Administrator), auf dem Computer *Canberra* beliebige Bildverarbeitungsgeräte (zum Beispiel eine Webcam) zu installieren, sofern signierte Treiber dafür vorhanden sind. Dabei ermitteln Sie zuerst die GUID der Setupklasse *Bildverarbeitungsgeräte* und konfigurieren dann die Computerrichtlinien so, dass Nicht-Administratoren diese Geräteklasse installieren dürfen. Für die Übung müssen Sie mindestens ein Gerät dieser Setupklasse auf Ihrem Computer installieren. Ist das nicht möglich, können Sie auch eine andere Setupklasse verwenden. Es geht nur darum, dass Sie sich mit dem Ablauf vertraut machen – die verwendete Gerätesetupklasse ist nicht wichtig. Gehen Sie folgendermaßen vor, um Nicht-Administratoren zu erlauben, ausgewählte Hardwaregerätetypen zu installieren:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Erstellen Sie das Standardbenutzerkonto *Don Hall*, sofern es noch nicht vorhanden ist.
3. Öffnen Sie den Geräte-Manager.
4. Erweitern Sie in der Strukturansicht des Geräte-Managers den Zweig *Bildverarbeitungsgeräte*. Wählen Sie ein Gerät aus (zum Beispiel eine Webcam).
5. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie den Befehl *Eigenschaften*.
6. Wählen Sie auf der Registerkarte *Details* in der Dropdownliste *Eigenschaft* den Eintrag *Geräteklasse-GUID* aus (Abbildung 4.23).

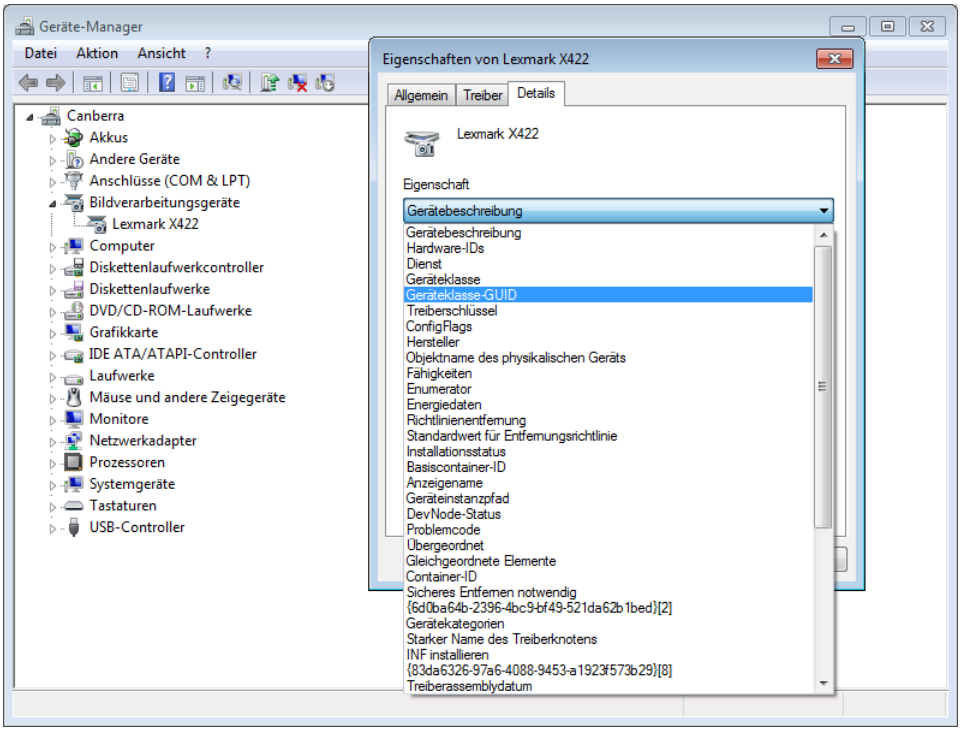


Abbildung 4.23 Ermitteln einer Geräteklassen-GUID

7. Die GUID wird nun angezeigt (Abbildung 4.24). Klicken Sie mit der rechten Maustaste auf die GUID und wählen Sie den Befehl *Kopieren*. Fügen Sie die GUID im Windows-Editor in eine neue Textdatei ein, Sie brauchen sie noch.

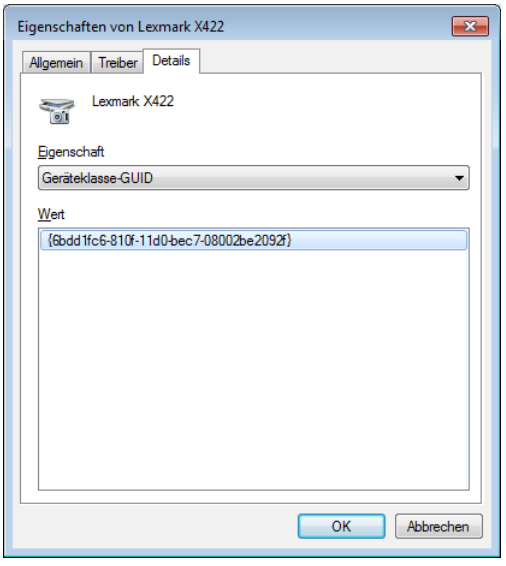


Abbildung 4.24 Die Geräteklassen-GUID für Bildverarbeitungsgeräte

8. Geben Sie im Suchfeld des Startmenüs **mmc gpedit.msc** ein und drücken Sie die EINGABETASTE. Daraufhin öffnet sich der Editor für lokale Gruppenrichtlinien.
9. Erweitern Sie im Editor für lokale Gruppenrichtlinien unter *Richtlinien für lokaler Computer* die Zweige *Computerkonfiguration*, *Administrative Vorlagen* und schließlich *System*. Wählen Sie den Knoten *Treiberinstallation* aus.
10. Klicken Sie in der Detailansicht doppelt auf *Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen* (Abbildung 4.25).

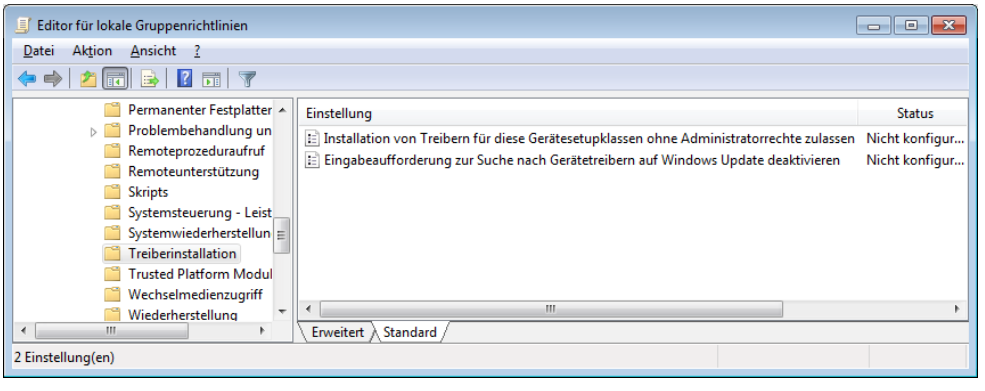


Abbildung 4.25 Öffnen der Richtlinie *Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen*

11. Wählen Sie im Dialogfeld *Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen* (Abbildung 4.26) die Option *Aktiviert* aus.

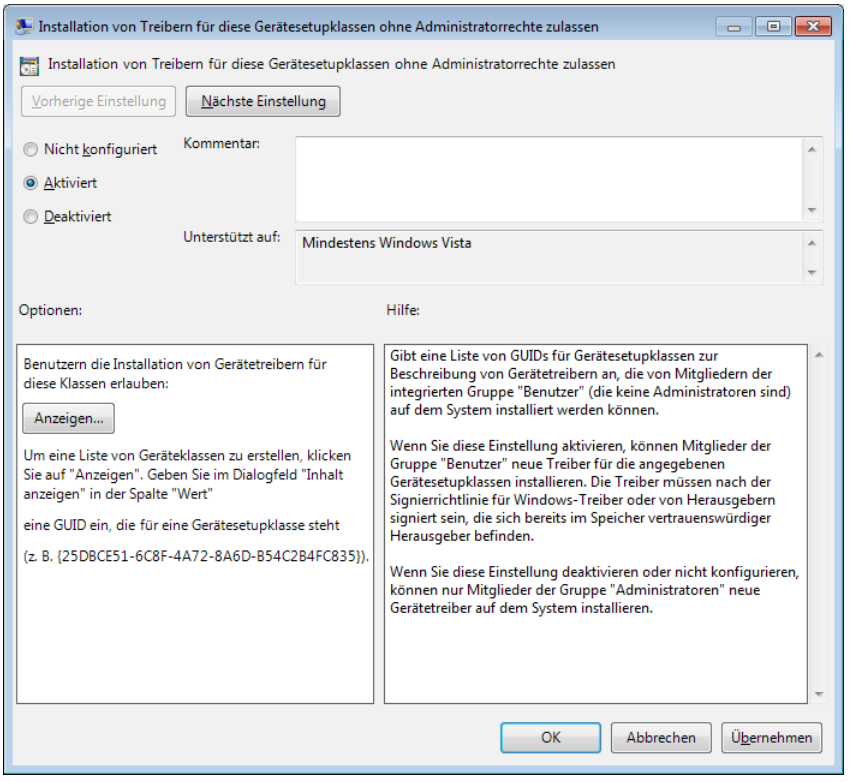

Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen
Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows Vista
Optionen:
Hilfe:
Benutzern die Installation von Gerätetreibern für diese Klassen erlauben:
Anzeigen...
Um eine Liste von Geräteklassen zu erstellen, klicken Sie auf "Anzeigen". Geben Sie im Dialogfeld "Inhalt anzeigen" in der Spalte "Wert"
eine GUID ein, die für eine Gerätesetupklasse steht
(z. B. {25DBCE51-6C8F-4A72-8A6D-B54C2B4FC835}).
Gibt eine Liste von GUIDs für Gerätesetupklassen zur Beschreibung von Gerätetreibern an, die von Mitgliedern der integrierten Gruppe "Benutzer" (die keine Administratoren sind) auf dem System installiert werden können.
Wenn Sie diese Einstellung aktivieren, können Mitglieder der Gruppe "Benutzer" neue Treiber für die angegebenen Gerätesetupklassen installieren. Die Treiber müssen nach der Signierrichtlinie für Windows-Treiber oder von Herausgebern signiert sein, die sich bereits im Speicher vertrauenswürdiger Herausgeber befinden.
Wenn Sie diese Einstellung deaktivieren oder nicht konfigurieren, können nur Mitglieder der Gruppe "Administratoren" neue Gerätetreiber auf dem System installieren.
OK
Abbrechen
Übernehmen

Abbildung 4.26 Aktivieren der Richtlinie *Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen*

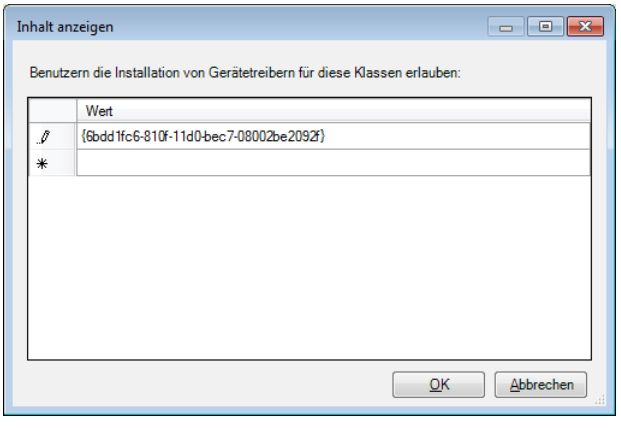


Abbildung 4.27 Einfügen der GUID in das Dialogfeld *Inhalt anzeigen*

12. Klicken Sie auf *Anzeigen*.
13. Wählen Sie im Dialogfeld *Inhalt anzeigen* das Textfeld in der Spalte *Wert* aus, klicken Sie doppelt in dieses Textfeld und fügen Sie die GUID ein, die Sie vorher kopiert haben (inklusive der geschweiften Klammern). Das Dialogfeld *Inhalt anzeigen* müsste nun wie in Abbildung 4.27 aussehen.
14. Klicken Sie auf *OK*, um das Dialogfeld *Inhalt anzeigen* zu schließen.
15. Klicken Sie auf *OK*, um das Dialogfeld *Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen* zu schließen. Der Editor für lokale Gruppenrichtlinien führt die Richtlinie nun als *Aktiviert* auf.
16. Wenn Sie wollen, können Sie nun den Treiber für das Bildverarbeitungsgerät eines zuverlässigen Herstellers bereitstellen. Melden Sie sich dann als *Don Hall* am Computer *Canberra* an und installieren Sie das Gerät. Übung 2 beschreibt, wie Sie einen Treiber bereitstellen.



Hinweis Treiber müssen signiert sein oder von einem Administrator genehmigt werden

Das Gerätetreiberpaket muss signiert sein, wie in den Computerrichtlinien festgelegt. Befindet sich das Zertifikat für den Treiber nicht im Zertifikatspeicher *Vertrauenswürdige Herausgeber*, wird der Benutzer während des Installationsvorgangs gefragt, ob er das ungeprüfte Zertifikat akzeptiert. Verfügt der Gerätetreiber nicht über eine gültige digitale Signatur, wird er nur installiert, wenn ein Administrator dies genehmigt.

Übung 2 Bereitstellen eines Gerätetreibers im Treiberspeicher

Wenn Sie Nicht-Administratoren erlaubt haben, Geräte einer bestimmten Gerätesetupklasse zu installieren, können Sie ihnen auch ermöglichen, ein bestimmtes Gerät dieser Klasse automatisch zu installieren, ganz so, als wäre es ein PnP-Gerät. Dazu stellen Sie den Treiber für dieses Gerät im Treiberspeicher bereit (das sogenannte Staging).

Der Treiberspeicher ist ein geschützter Bereich, der alle Gerätetreiberpakete enthält, deren Installation auf dem Computer genehmigt wurde. Befindet sich ein Gerätetreiberpaket im Treiberspeicher, kann ein Standardbenutzer des Computers das entsprechende Gerät ohne erhöhte Benutzerprivilegien installieren. Gehen Sie folgendermaßen vor, um ein Treiberpaket im Treiberspeicher bereitzustellen:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Kopieren Sie den Treiber von dem Medium, das der Hersteller seinem Gerät beigelegt hat, in einen Ordner auf Ihrer Festplatte, etwa *C:\Newdrivers*. In dieser Übung nehmen wir an, dass der Treiber den Namen *Mydriver.inf* trägt.
3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Klicken Sie bei Bedarf auf *Ja*, um das UAC-Dialogfeld zu bestätigen.
4. Geben Sie **pnputil -a c:\newdrivers\mydriver.inf** ein (passen Sie diesen Befehl an, wenn Sie einen anderen Pfad oder Dateinamen verwenden).
5. Falls das Treiberpaket unsigniert ist oder mit einem Zertifikat signiert wurde, das momentan nicht im Zertifikatspeicher *Vertrauenswürdige Herausgeber* aufgeführt ist, öffnet sich das Dialogfeld *Windows-Sicherheit*, in dem Sie gefragt werden, ob Sie den Treiber wirklich installieren wollen. Sehen Sie sich die Einzelheiten dieser Meldung

an, um festzustellen, welches Problem mit der Signatur des Treibers vorliegt. Klicken Sie auf *Installieren*, wenn Sie sicher sind, dass das Treiberpaket vertrauenswürdig ist. Damit ist das Staging abgeschlossen.

6. Sobald der Treiber bereitgestellt ist, meldet das Tool PnPUtil einen veröffentlichten Namen (*oem<Zahl>.inf*), den Windows 7 diesem Paket im Treiberspeicher zuweist. Sie müssen diesen Namen angeben, wenn Sie das Treiberpaket später wieder aus dem Speicher löschen wollen. Sie können den veröffentlichten Namen für ein Treiberpaket auch jederzeit ermitteln, indem Sie **pnputil.exe -e** eingeben und nach dem gewünschten Treiber suchen.



Weitere Informationen Das Tool PnPUtil

Weitere Informationen über das Tool PnPUtil finden Sie unter *http://technet.microsoft.com/en-us/library/cc732408.aspx*.

Übung 3 Windows 7 so konfigurieren , dass es in zusätzlichen Ordnern nach Gerätetreibern sucht

Wenn ein neues Gerät an einen Computer angeschlossen wird, durchsucht Windows 7 den Treiberspeicher, um festzustellen, ob ein geeignetes Treiberpaket bereitgestellt wurde. Ist das nicht der Fall, sucht es an mehreren Orten nach einem Treiberpaket, das es in den Treiberspeicher kopieren kann. Diese Orte sind:

- Die Ordner, die im Registrierungseintrag *DevicePath* angegeben sind
- Die Windows Update-Website. Beachten Sie, dass Sie diese Internetsuche im Editor für lokale Gruppenrichtlinien verhindern können, indem Sie den Zweig *Richtlinien für lokaler Computer/Computerkonfiguration/Administrative Vorlagen/System/Internetkommunikationsverwaltung/Internetkommunikationseinstellungen* öffnen und die Einstellung *Suche nach Gerätetreibern auf Windows Update deaktivieren* konfigurieren.
- Ein Dateipfad (normalerweise auf einem Wechseldatenträger), den der Benutzer angibt

Gehen Sie folgendermaßen vor, um die Liste der Ordner zu ändern, in denen der Geräte-Manager nach einem Treiberpaket sucht:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Geben Sie im Suchfeld des Startmenüs **regedit** ein. Klicken Sie bei Bedarf auf *Ja*, um das UAC-Dialogfeld zu bestätigen.
3. Wählen Sie den folgenden Registrierungsschlüssel aus:

   `HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion`
4. Klicken Sie in der Detailansicht doppelt auf *DevicePath*.
5. Fügen Sie weitere Ordnerpfade zu diesem Eintrag hinzu. Trennen Sie die Ordnerpfade dabei mit einem Strichpunkt (Abbildung 4.28). Stellen Sie sicher, dass Sie *%SystemRoot%\Inf* nicht löschen.

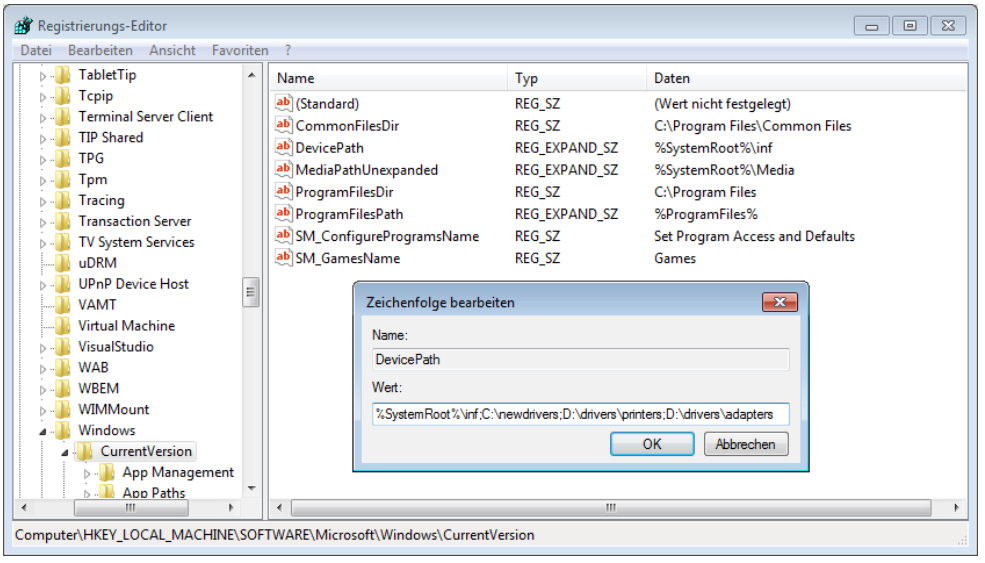


Abbildung 4.28 Bearbeiten des Registrierungseintrags *DevicePath*



Hinweis **Unterordner von *DevicePath***

Wenn die Ordner, die Sie im Registrierungseintrag *DevicePath* eintragen, Unterordner enthalten, werden auch diese Unterordner in die Suche einbezogen. Tragen Sie beispielsweise *C:* als Pfad ein, durchsucht Windows das gesamte Laufwerk (was vermutlich längere Zeit dauert).

Zusammenfassung der Lektion

- Ein Nicht-Administrator kann PnP-Geräte installieren, wenn deren Treiber eine gültige digitale Signatur hat, die mit Zertifikaten im Speicher *Vertrauenswürdige Herausgeber* verknüpft ist. Wenn sich der Gerätetreiber nicht im Gerätetreiberspeicher befindet, unsigniert ist oder die Signatur nicht als vertrauenswürdig eingestuft wird, muss ein Administrator die Installation des Geräts genehmigen.
- Ein Administrator kann die Installation eines Geräts ermöglichen, indem er seinen Treiber im Gerätetreiber bereitstellt. Ist der Gerätetreiber unsigniert, kann der Administrator ihn selbst mit einem Zertifikat signieren, das von einer internen Zertifizierungsstelle stammt. So können Standardbenutzer innerhalb einer Organisation das Gerät installieren.
- Sie können verhindern, dass Treiber von Windows Update heruntergeladen und automatisch installiert werden. Sie können Windows Update auch aus dem Suchpfad für Gerätetreiber entfernen. Sie können Treiber deaktivieren oder beenden, um Treiberprobleme zu diagnostizieren. Falls bei einem neuen Treiber Probleme auftreten, können Sie die vorherige Version wiederherstellen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Verwalten von Gerätetreibern und Geräten«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Ein Benutzer ohne Administratorprivilegien schließt ein Gerät an einen Windows 7-Computer an. Welche der folgenden Voraussetzungen müssen erfüllt sein, damit er das Gerät installieren kann? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Der Gerätetreiber muss eine gültige digitale Signatur haben.
   B. Der Gerätetreiber muss im Speicher *Vertrauenswürdige Herausgeber* abgelegt sein.
   C. Der Gerätetreiber muss im Gerätetreiberspeicher bereitgestellt sein.
   D. Das Gerät muss über einen USB-Anschluss verbunden sein.
   E. Der Gerätetreiber muss von Microsoft signiert sein.
2. Sie haben vier Geräte an einen USB-Hub angeschlossen. Keines davon funktioniert besonders gut. Sie vermuten, dass eines der Geräte mehr Bandbreite benötigt und nicht über einen Hub angeschlossen sein sollte. Wie ermitteln Sie die Bandbreitenanforderungen der Geräte?
   A. Klicken Sie im Geräte-Manager doppelt auf *USB-Controller*, klicken Sie mit der rechten Maustaste auf den Hostcontroller Ihres Systems und wählen Sie den Befehl *Eigenschaften*. Öffnen Sie die Registerkarte *Stromversorgung*.
   B. Klicken Sie im Geräte-Manager doppelt auf *USB-Controller*, klicken Sie mit der rechten Maustaste auf den Hostcontroller Ihres Systems und wählen Sie den Befehl *Eigenschaften*. Öffnen Sie die Registerkarte *Erweitert*.
   C. Klicken Sie im Geräte-Manager doppelt auf *Eingabegeräte (Human Interface Devices)* und klicken Sie nacheinander jeweils mit der rechten Maustaste auf jedes USB-Eingabegerät. Öffnen Sie zu jedem Gerät die Registerkarte *Details*.
   D. Klicken Sie im Geräte-Manager doppelt auf *IEEE 1394 Bus-Hostcontroller* und klicken Sie nacheinander jeweils mit der rechten Maustaste auf jedes Gerät. Öffnen Sie zu jedem Gerät die Registerkarte *Ressourcen*.
3. Sie wollen es normalen Benutzern ermöglichen, ein Gerät zu installieren. Der Gerätetreiber hat eine gültige digitale Signatur, deren Zertifikat im Speicher *Vertrauenswürdige Herausgeber* eingetragen ist. Wie stellen Sie sicher, dass Nicht-Administratoren das Gerät installieren können? (Wählen Sie alle zutreffenden Antworten aus; sie bilden zusammen die richtige Lösung.)
   A. Klicken Sie im Geräte-Manager doppelt auf den Gerätetyp, klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie den Befehl *Eigenschaften*. Ermitteln Sie auf der Registerkarte *Details* die Geräteklasse-GUID. Aktivieren Sie

im Gruppenrichtlinieneditor die Richtlinie *Installation von Treibern für diese Gerätesetupklassen ohne Administratorrechte zulassen* und tragen Sie die GUID ein.

B. Öffnen Sie den Registrierungsschlüssel *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion* und klicken Sie in der Detailansicht doppelt auf *DevicePath*. Fügen Sie das Laufwerk *C:* zum Suchpfad hinzu.

C. Stellen Sie den Gerätetreiber bereit, indem Sie ihn in den Speicher *Vertrauenswürdige Herausgeber* kopieren.

D. Stellen Sie den Gerätetreiber bereit, indem Sie ihn in den Gerätetreiber kopieren.

4. Sie wollen verhindern, dass Windows 7 in Windows Update nach einem Gerätetreiber sucht, wenn kein Treiber im Gerätetreiberspeicher vorhanden ist. Wie gehen Sie vor?

   A. Wählen Sie im Dialogfeld *Geräteinstallationseinstellungen* statt *Ja, automatisch ausführen (empfohlen)* die Option *Nein, zu installierende Software selbst auswählen* und dann *Nie Treibersoftware von Windows Update installieren* aus. Klicken Sie auf *Änderungen speichern*.

   B. Wählen Sie im Editor für lokale Gruppenrichtlinien den Zweig *Richtlinien für lokaler Computer/Computerkonfiguration/Administrative Vorlagen/System/Internetkommunikationsverwaltung/Internetkommunikationseinstellungen* aus und konfigurieren Sie die Einstellung *Suche nach Gerätetreibern auf Windows Update deaktivieren*.

   C. Öffnen Sie den Registrierungsschlüssel *HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion* und klicken Sie in der Detailansicht doppelt auf *DevicePath*. Entfernen Sie Windows Update aus dem Suchpfad.

   D. Wählen Sie im Dialogfeld *Geräteinstallationseinstellungen* statt *Ja, automatisch ausführen (empfohlen)* die Option *Nein, zu installierende Software selbst auswählen* und dann *Immer die beste Treibersoftware von Windows Update installieren* aus. Klicken Sie auf *Änderungen speichern*.

5. Sie vermuten, dass ein Gerät, das im Geräte-Manager unter *Nicht-PnP-Treiber* aufgeführt ist, Probleme verursacht. Wie können Sie das Gerät sofort beenden, um die Probleme zu analysieren?

   A. Öffnen Sie im Geräte-Manager das Eigenschaftendialogfeld des Geräts. Klicken Sie auf der Registerkarte *Treiber* auf *Beenden*.

   B. Öffnen Sie im Geräte-Manager das Eigenschaftendialogfeld des Geräts. Ändern Sie den Starttyp auf der Registerkarte *Treiber* auf *Deaktiviert*.

   C. Öffnen Sie im Geräte-Manager das Eigenschaftendialogfeld des Geräts. Klicken Sie auf der Registerkarte *Treiber* auf *Deaktivieren*.

   D. Öffnen Sie im Geräte-Manager das Eigenschaftendialogfeld des Geräts. Klicken Sie auf der Registerkarte *Treiber* auf *Deinstallieren*.

Lektion 2: Verwalten von Datenträgern

Windows 7 bietet eine ganze Reihe von Möglichkeiten für die Verwaltung von Datenträgern. Sie können nicht benötigte oder unerwünschte Dateien automatisch von Ihrer Festplatte löschen und die Datenzugriffszeiten durch regelmäßige *Defragmentierung* verbessern, damit Dateien in fortlaufenden Bereichen der Festplatte gespeichert sind.

Sie können Basis- und dynamische Datenträger bearbeiten und Festplatten in dynamische Datenträger, GPT-Datenträger (GUID Partition Table) und MBR-Datenträger (Master Boot Record) konvertieren. Sie können Volumes vergrößern oder verkleinern, und Sie können übergreifende oder Stripesetpartitionen verwenden. Windows 7 führt neue Fähigkeiten im Bereich von externen USB-Datenträgern und USB-Flashsticks ein, die in den Vorversionen nicht zur Verfügung standen. Sie können Systempartitionen auf USB-Wechseldatenträgern installieren und den Computer davon starten.

Wenn Sie mehrere Festplattenlaufwerke haben, können Sie *RAID-Systeme* (Redundant Array of Independent Disks) implementieren, um die Leistung zu verbessern, Daten zu schützen oder beides. Sie können Stripsets, Spiegelung oder Stripesets mit Parity implementieren. Sie können Volumes verkleinern und vergrößern, ohne auf Tools anderer Hersteller zurückgreifen zu müssen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Durchführen von Datenträgerbereinigung und Defragmentierung
- Verwalten von Datenträgern mit Diskpart und der Datenträgerverwaltung
- Verwalten von Wechseldatenträgern
- Verwalten von Datenträgervolumes und Partitionen, inklusive RAID-Volumes

Veranschlagte Zeit für diese Lektion: 50 Minuten

Datenträgerwartung

Bevor wir uns ansehen, welche Möglichkeiten Windows 7 zur Verfügung stellt, um Datenträger zu bearbeiten und zu verwalten, müssen Sie sich über die grundlegenden Prinzipien im Klaren sein. Jedes Datenträgersystem funktioniert am besten, wenn es nicht mit unnötigen Dateien vollgestopft ist und die Dateien fortlaufend auf der Platte liegen, also keine Fragmente in unterschiedlichen physischen Bereichen der Plattenoberfläche abgelegt sind. Daher können Sie die Leistung praktisch immer verbessern, indem Sie eine Datenträgerbereinigung ausführen und Ihre Festplatten regelmäßig defragmentieren.

Verwenden der Datenträgerbereinigung

Die Datenträgerbereinigung löscht nicht benötigte Dateien, zum Beispiel Dateien, die Sie heruntergeladen haben, um Programme zu installieren, temporäre Internetdateien, Dateien im Papierkorb, Offlinewebseiten, Ruhezustandsdateien, Setupprotokolldateien, temporäre Dateien und Vorschaubilder. Im Dialogfeld *Datenträgerbereinigung* (Abbildung 4.29) legen Sie fest, welche Dateien von der ausgewählten Festplatte gelöscht werden. Standardmäßig ausgewählt sind *Heruntergeladene Programmdateien*, *Temporäre Internetdateien* und *Miniaturansichten*. Am einfachsten starten Sie dieses Tool, indem Sie im Suchfeld des Startmenüs **Datenträgerbereinigung** eingeben.

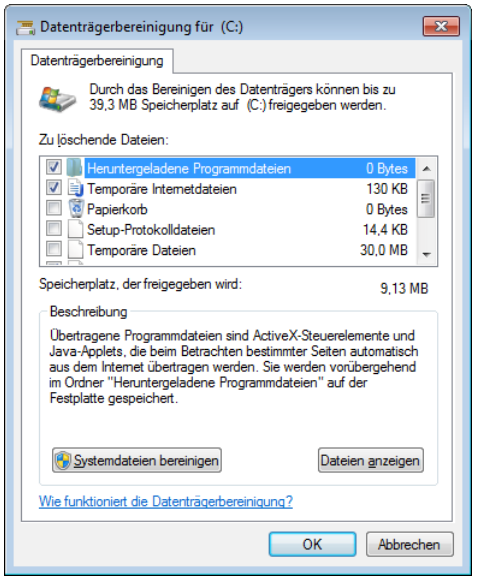

Datenträgerbereinigung für (C:)
Datenträgerbereinigung
Durch das Bereinigen des Datenträgers können bis zu 39,3 MB Speicherplatz auf (C:) freigegeben werden.
Zu löschende Dateien:
Heruntergeladene Programmdateien 0 Bytes
Temporäre Internetdateien 130 KB
Papierkorb 0 Bytes
Setup-Protokolldateien 14,4 KB
Temporäre Dateien 30,0 MB
Speicherplatz, der freigegeben wird: 9,13 MB
Beschreibung
Übertragene Programmdateien sind ActiveX-Steuerelemente und Java-Applets, die beim Betrachten bestimmter Seiten automatisch aus dem Internet übertragen werden. Sie werden vorübergehend im Ordner "Heruntergeladene Programmdateien" auf der Festplatte gespeichert.
Systemdateien bereinigen
Dateien anzeigen
Wie funktioniert die Datenträgerbereinigung?
OK
Abbrechen

Abbildung 4.29 Die Datenträgerbereinigung

Eine Beschreibung zu allen verfügbaren Elementen erhalten Sie, indem Sie das Element auswählen. Wenn Sie das Kontrollkästchen neben einem Element aktivieren, werden die zugehörigen Dateien für die Löschung vorgesehen. Sie können auf *Dateien anzeigen* klicken, um Einzelheiten über die Dateien zu erhalten. Das hilft bei der Entscheidung, ob Sie die Dateien wirklich löschen wollen.

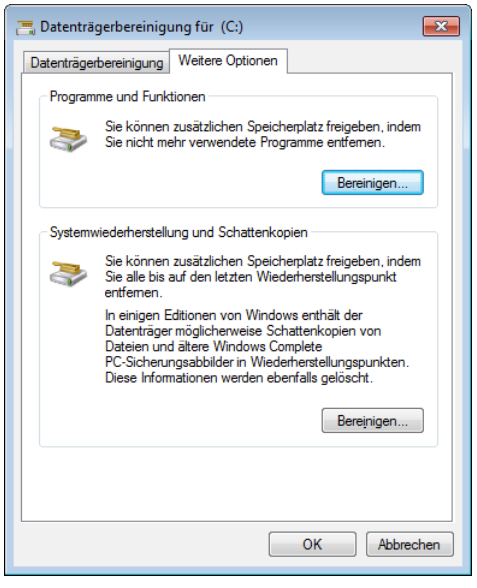

Datenträgerbereinigung für (C:)
Datenträgerbereinigung
Weitere Optionen
Programme und Funktionen
Sie können zusätzlichen Speicherplatz freigeben, indem Sie nicht mehr verwendete Programme entfernen.
Bereinigen...
Systemwiederherstellung und Schattenkopien
Sie können zusätzlichen Speicherplatz freigeben, indem Sie alle bis auf den letzten Wiederherstellungspunkt entfernen.
In einigen Editionen von Windows enthält der Datenträger möglicherweise Schattenkopien von Dateien und ältere Windows Complete PC-Sicherungsabbilder in Wiederherstellungspunkten. Diese Informationen werden ebenfalls gelöscht.
Bereinigen...
OK
Abbrechen

Abbildung 4.30 Die Registerkarte *Weitere Optionen* der Datenträgerbereinigung

Wenn Sie die verschiedenen Dateitypen ausgewählt haben, die Sie löschen wollen, und auf *OK* klicken, werden Sie in einem Dialogfeld gefragt, ob die Dateien wirklich für immer gelöscht werden sollen. Sobald Sie auf *Dateien löschen* klicken, werden die Dateien gelöscht.

Ein Standardbenutzer ohne Administratorprivilegien kann mit der Datenträgerbereinigung einfache Dateien löschen. Wollen Sie allerdings Systemdateien löschen, indem Sie auf die Schaltfläche *Systemdateien bereinigen* klicken, müssen Sie als Administrator angemeldet sein oder Administratoranmeldeinformationen eingeben. In diesem Fall wird die Systembereinigung automatisch ausgeführt. Das Tool Datenträgerbereinigung entfernt die Schaltfläche *Systemdateien bereinigen* und Sie haben Zugriff auf die Registerkarte *Weitere Optionen* (Abbildung 4.30), in der weitere Aufräumoperationen verfügbar sind.

Defragmentieren von Festplatten

Sie können interne und externe Festplatten, USB-Flashsticks und virtuelle Festplatten (VHDs) defragmentieren. Wenn Ihre Festplatte oder Ihr Speichergerät fragmentiert ist, kann das die Leistung Ihres Computers verschlechtern. Bei der Defragmentierung werden fragmentierte Daten auf Ihrem Datenträger so angeordnet, dass die Laufwerke wieder effizienter arbeiten. Normalerweise wird die Defragmentierung nach einem regelmäßigen Zeitplan ausgeführt, aber Sie können die Analyse und Defragmentierung Ihrer Datenträger und Laufwerke auch von Hand anstoßen.

Das Tool zeigt alle Datenträger und Speichergeräte auf dem Computer an, die defragmentiert werden können. Wählen Sie ein Laufwerk aus und klicken Sie auf *Datenträger analysieren*, um den aktuellen Fragmentierungsgrad zu ermitteln und festzustellen, ob es defragmentiert werden sollte. Sie müssen unter einem Administratorkonto angemeldet sein oder Administratoranmeldeinformationen eingeben, um einen Datenträger zu analysieren (und zu defragmentieren). Ergibt die Analyse einen Fragmentierungsgrad von 10 Prozent oder mehr, sollten Sie den Datenträger defragmentieren, indem Sie auf *Datenträger defragmentieren* klicken.

Die Datenträgerdefragmentierung dauert einige Minuten bis mehrere Stunden, je nach Größe und Fragmentierungsgrad der Festplatte. Sie können mit Ihrem Computer weiterarbeiten, während der Defragmentierungsprozess läuft.

Sie können eine regelmäßige Datenträgerdefragmentierung einplanen, indem Sie auf *Zeitplan konfigurieren* klicken. Das Dialogfeld *Defragmentierung: Zeitplan ändern* sehen Sie in Abbildung 4.31. In der Standardeinstellung werden die Datenträger einmal wöchentlich am Mittwoch um 1:00 Uhr nachts defragmentiert. Sie können das in den Dropdownlisten ändern. In der Standardeinstellung werden alle Datenträger defragmentiert, auch neue Datenträger, die hinzugefügt werden. Das können Sie bei Bedarf ändern, indem Sie auf *Datenträger auswählen* klicken.

Über das Tool Datenträgerdefragmentierung können Sie auf einem Computer nur einen einzigen Zeitplan für die Datenträgerdefragmentierung einrichten. Ist ein Datenträger aus dem Zeitplan ausgeschlossen, wird er nicht defragmentiert, sofern Sie das nicht von Hand anstoßen. Wenn ein Datenträger ausschließlich von einem anderen Programm benutzt wird oder mit einem anderen Dateisystem als NTFS formatiert ist, kann er nicht defragmentiert werden. Auch Netzwerkspeicherorte können nicht defragmentiert werden.

Ein Datenträger kann sehr schnell stark fragmentiert werden, wenn er viel benutzt wird und häufig Daten darauf geschrieben werden. Abbildung 4.32 (die Sie auch in den Testfragen auf der Begleit-CD finden) zeigt genau eine solche Situation. Laufwerk *C:* wurde binnen lediglich 6 Tagen stark fragmentiert und drückt bereits die Leistung des Computers. Das Problem

lässt sich einstweilen beseitigen, indem Sie die Festplatte von Hand defragmentieren, aber dann wird es nicht lange dauern, bis sie erneut fragmentiert ist. Die sinnvolle Lösung besteht daher darin, den Zeitplan so zu ändern, dass die Festplatte öfter defragmentiert wird.

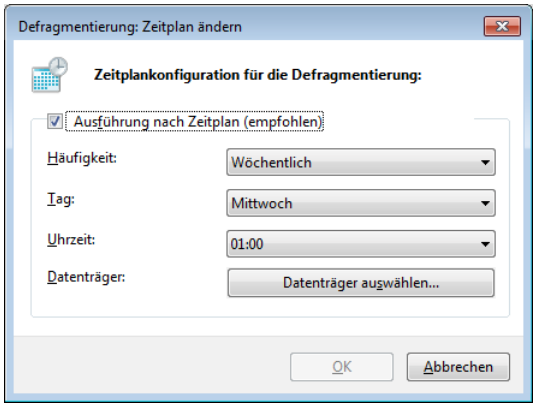


Abbildung 4.31 Konfiguration des Zeitplans für die Datenträgerdefragmentierung

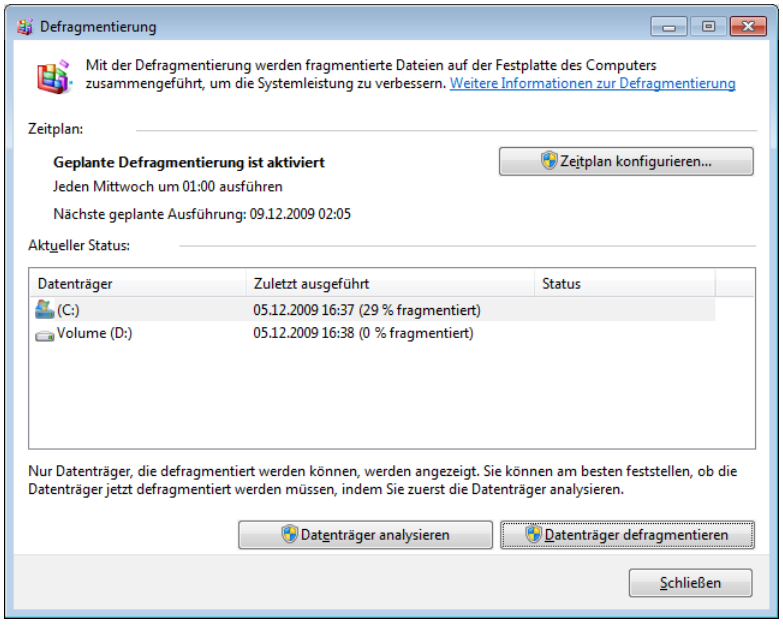

Defragmentierung
Mit der Defragmentierung werden fragmentierte Dateien auf der Festplatte des Computers zusammengeführt, um die Systemleistung zu verbessern. Weitere Informationen zur Defragmentierung
Zeitplan:
Geplante Defragmentierung ist aktiviert
Jeden Mittwoch um 01:00 ausführen
Nächste geplante Ausführung: 09.12.2009 02:05
Zeitplan konfigurieren...
Aktueller Status:
Datenträger
Zuletzt ausgeführt
Status
(C:)
05.12.2009 16:37 (29 % fragmentiert)
Volume (D:)
05.12.2009 16:38 (0 % fragmentiert)
Nur Datenträger, die defragmentiert werden können, werden angezeigt. Sie können am besten feststellen, ob die Datenträger jetzt defragmentiert werden müssen, indem Sie zuerst die Datenträger analysieren.
Datenträger analysieren
Datenträger defragmentieren
Schließen

Abbildung 4.32 Eine stark fragmentierte Festplatte

Sie können einen Datenträger auch defragmentieren, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten das Befehlszeilentool Defrag aufrufen. Defrag hat die folgende Syntax:

```
Defrag <Volume> | /C | /E <Volumes> [/A | /X | /T] [/H] [/M] [/U] [/V]
```



Prüfungstipp

Die Syntax von Defrag hat sich gegenüber Windows Vista verändert. In den Prüfungen werden häufig Dinge behandelt, die sich geändert haben.

Die Argumente von Defrag haben folgende Bedeutung:

- ***<Volume>*** Der Laufwerkbuchstabe oder Bereitstellungspunkt des Volumes, das defragmentiert werden soll
- **/C** Defragmentiert alle lokalen Volumes auf dem Computer.
- **/E** Defragmentiert alle lokalen Volumes auf dem Computer, außer den angegebenen.
- **/A** Zeigt einen Bericht mit einer Fragmentierungsanalyse für das angegebene Volume an, ohne es zu defragmentieren. Der Analysebericht nennt Volumegröße, freien Speicherplatz, insgesamt fragmentierten Speicherplatz und Größe des längsten freien Bereichs. Außerdem erfahren Sie darin, ob Sie das Volume defragmentieren sollten.
- **/X** Fasst den freien Speicherplatz fortlaufend zusammen. Das ist nützlich, wenn Sie ein Volume verkleinern wollen. Außerdem verringert sich dadurch die Fragmentierung neuer Dateien.
- **/T** Überwacht eine Operation, die bereits auf dem angegebenen Volume ausgeführt wird.
- **/H** Führt die Operation mit normaler Priorität aus, statt wie in der Standardeinstellung mit geringer Priorität. Verwenden Sie dieses Argument, wenn der Computer gerade nicht anderweitig ausgelastet ist.
- **/M** Defragmentiert mehrere Volumes gleichzeitig, also parallel. Dieses Argument können Sie auf Computern verwenden, die auf mehrere Datenträger gleichzeitig zugreifen. Dies ist möglich, wenn der Computer beispielsweise mit SCSI- (Small Computer System Interface) oder SATA-Festplatten (Serial Advanced Technology Attachment) ausgestattet ist statt mit IDE-Festplatten (Integrated Drive Electronics).
- **/U** Zeigt den Fortschritt der Operation auf dem Bildschirm an.
- **/V** Ausführlicher Modus. Liefert zusätzliche Details und Statistiken.

Zum Beispiel defragmentiert der Befehl `defrag /c /h /u` alle Festplatten und Speichergeräte auf dem Computer, bei denen das sinnvoll ist, und zeigt den Fortschritt in der Eingabeaufforderung an. Der Befehl liefert zu jeder Festplatte und jedem Gerät einen Bericht, der den Zustand vor der Defragmentierung beschreibt, liefert Details zu den Defragmentierungsdurchgängen, fasst automatisch den freien Platz zusammen und erstellt einen Bericht über den Zustand nach Abschluss der Defragmentierung. Er läuft mit normaler Priorität, sodass er schneller beendet ist, aber Sie sollten das Argument `/H` vermeiden, wenn Sie gleichzeitig andere Arbeiten mit dem Computer erledigen wollen.



Hinweis Ausgabe von Defrag

Die Ausgabe des Befehls `defrag /c /h /u` ist so ausführlich, dass sie nicht in eine Abbildung passt. Sie können sich den Text ansehen, indem Sie den Befehl selbst auf Ihrem Computer ausführen.

Überprüfen einer Festplatte auf Fehler

Falls eine Festplatte nicht im Tool Datenträgerdefragmentierung aufgelistet wird, obwohl sie vorhanden sein müsste, hat sie möglicherweise einen Defekt. Sie können Computerprobleme beseitigen und die Leistung des Computers verbessern, indem Sie Ihre Festplatte auf Fehler überprüfen. Viele Fehlerarten kann Windows 7 automatisch reparieren. Gehen Sie folgendermaßen vor, um eine Festplatte auf Fehler zu überprüfen:

1. Klicken Sie im Startmenü auf *Computer*.
2. Klicken Sie mit der rechten Maustaste auf die Festplatte, die Sie überprüfen wollen, und wählen Sie den Befehl *Eigenschaften*.
3. Klicken Sie auf der Registerkarte *Tools* im Abschnitt *Fehlerüberprüfung* auf *Jetzt prüfen*.
4. Aktivieren Sie das Kontrollkästchen *Dateisystemfehler automatisch korrigieren*, wenn Sie erkannte Probleme automatisch reparieren wollen. Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird der Datenträger auf Fehler überprüft, sie werden aber nicht repariert.
5. Aktivieren Sie das Kontrollkästchen *Fehlerhafte Sektoren suchen/wiederherstellen*, wenn Sie die Festplatte gründlich überprüfen wollen. Diese Überprüfung versucht, Hardwarefehler auf der Festplatte selbst zu finden und zu reparieren. Beachten Sie aber, dass dies sehr lange dauern kann. Abbildung 4.33 zeigt das Dialogfeld der Datenträgerprüfung, in dem beide Kontrollkästchen aktiviert sind.

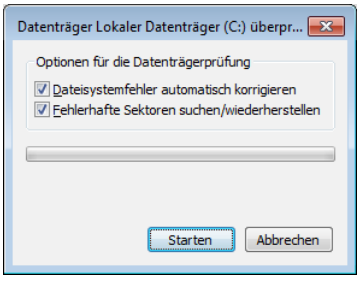


Abbildung 4.33 Überprüfen einer Festplatte nach Datei- und Hardwarefehlern

6. Klicken Sie auf *Starten*.
7. Sofern Sie *Dateisystemfehler automatisch korrigieren* aktiviert und einen Datenträger ausgewählt haben, der gerade benutzt wird (beispielsweise die Partition, die Windows enthält), werden Sie aufgefordert, die Datenträgerprüfung für den nächsten Neustart Ihres Computers einzuplanen. Stellen Sie in diesem Fall sicher, dass Sie alle Dokumente gespeichert und alle Fenster geschlossen haben, bevor Sie den Computer neu starten.

Einstellen von Datenträgerrichtlinien mit dem Editor für lokale Gruppenrichtlinien

Wechseldatenträger sind bequem, aber unter Umständen gefährden sie die Sicherheit. Werden vertrauliche Unternehmensdaten auf einem USB-Flashstick gespeichert, können sie leicht verloren gehen oder gestohlen werden. Das gilt genauso für Daten, die auf einen MP3-Player oder ein Handy heruntergeladen werden. Wenn der Computer CDs oder DVDs brennt, können

auch diese optischen Medien in die falschen Hände gelangen (wenn Sie sie zum Beispiel als Lesezeichen verwenden und dann in einer Bibliothek verlieren).

Statt die Daten mit BitLocker zu schützen, können Sie Benutzern ganz verbieten, Daten auf Wechseldatenträger zu schreiben. Sie können auch verhindern, dass Benutzer Daten herunterladen und Software ausführen, die auf Wechseldatenträgern gespeichert ist, weil in diesem Fall die Gefahr besteht, dass Malware auf den Computer gelangt.

Auf einem eigenständigen Clientcomputer können Sie diese Konfiguration im Editor für lokale Gruppenrichtlinien vornehmen. In einem Unternehmen bearbeiten Sie üblicherweise Domänengruppenrichtlinien auf einem Domänencontroller und wenden sie auf alle Clients in der Domäne an. Erweitern Sie im Editor für lokale Gruppenrichtlinien die Zweige *Computerkonfiguration*, *Administrative Vorlagen* und *System* und klicken Sie auf *Wechselmedienzugriff*. Abbildung 4.34 zeigt, welche Richtlinien Sie hier konfigurieren können. Mit »WPD-Geräte« sind Handys, Mediaplayer, zusätzliche Bildschirme, CE-Geräte und ähnliche Geräte gemeint.

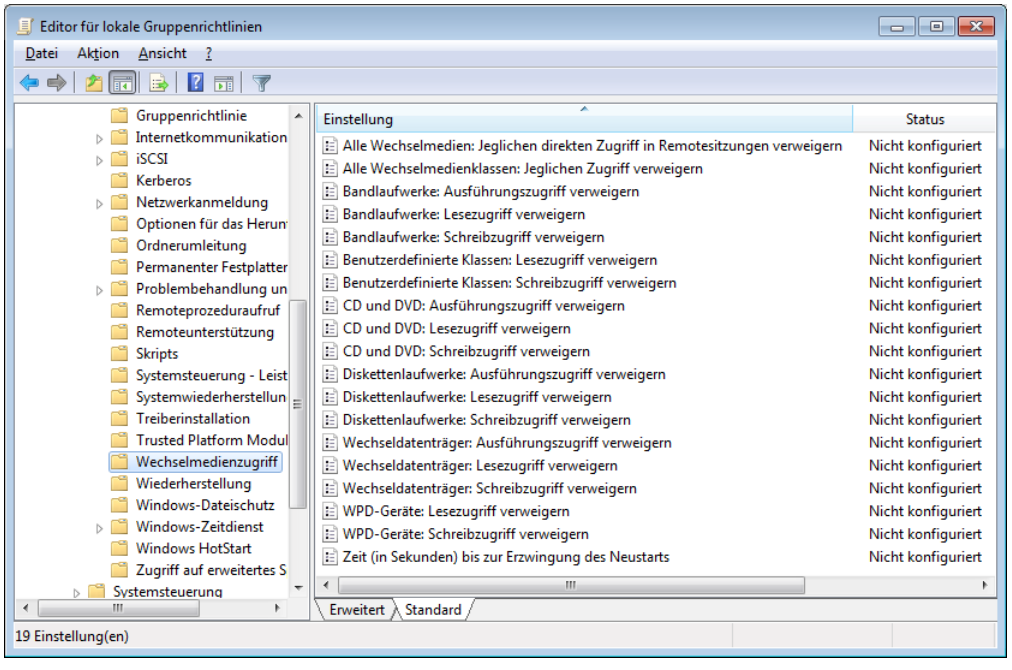


Abbildung 4.34 Konfigurierbare Richtlinien steuern die Verwendung von Wechseldatenträgern

Sie können folgende Richtlinien aktivieren, deaktivieren oder anderweitig konfigurieren:

- *Zeit (in Sekunden) bis zur Erzwingung des Neustarts*
- *CD und DVD: Ausführungs-, Lese- oder Schreibzugriff verweigern*
- *Benutzerdefinierte Klassen: Lese- oder Schreibzugriff verweigern*
- *Diskettenlaufwerke: Ausführungs-, Lese- oder Schreibzugriff verweigern*
- *Wechseldatenträger: Ausführungs-, Lese- oder Schreibzugriff verweigern*
- *Alle Wechselmedienklassen: Jeglichen Zugriff verweigern*

- *Alle Wechselmedien: Jeglichen direkten Zugriff in Remotesitzungen verweigern*
- *Bandlaufwerke: Ausführungs-, Lese- oder Schreibzugriff verweigern*
- *WPD-Geräte: Lese- oder Schreibzugriff verweigern*

Die meisten dieser Richtlinien sind selbsterklärend. Wenn Sie beispielsweise die Richtlinie *Zeit (in Sekunden) bis zur Erzwingung des Neustarts* aktivieren, müssen Sie angeben, wie lange bis zum Neustart des Systems gewartet wird. Wenn Sie diese Einstellung deaktivieren oder nicht konfigurieren, erzwingt das System keinen Neustart, sodass alle Richtlinien für Zugriffsrechte, die Sie konfigurieren, erst dann wirksam werden, wenn das System das nächste Mal neu gestartet wird. Indem Sie die Richtlinien zu benutzerdefinierten Klassen konfigurieren, können Sie Wechselmedienklassen durch Eingabe der Klassen-GUID auswählen.

Die Richtlinien für Wechseldatenträger betreffen nicht CDs, DVDs oder Disketten. Normalerweise werden sie benutzt, um den Zugriff auf USB-Flashstick, tragbare Mediaplayer und Handys zu steuern. Wenn Sie allerdings die Richtlinie *Alle Wechselmedien: Jeglichen Zugriff verweigern* aktivieren, werden Ausführungs-, Lese- und Schreibberechtigungen für alle Arten von Wechseldatenträgern verweigert; diese Einstellung hat Vorrang vor allen anderen konfigurierten Richtlinien, die Zugriffsrechte auf Wechseldatenträger betreffen. Wenn Sie die Richtlinie *Alle Wechselmedien: Jeglichen direkten Zugriff in Remotesitzungen verweigern* [richtig: *zulassen*] aktivieren, können Remotebenutzer in einer Sitzung auf Wechselmediengeräte zugreifen. (Die Richtlinie heißt im englischen *All Removable Storage: Allow direct access in remote sessions«*, also *zulassen*.)

Eine ausführliche Schritt-für-Schritt-Anleitung, wie Sie Downloads auf USB-Flashstick verhindern, finden Sie in den Übungen weiter unten in dieser Lektion.

Ändern von Datenträgertyp und Partitionsstil

Kapitel 2, »Konfigurieren von Systemabbildern«, hat die Konsole *Datenträgerverwaltung* vorgestellt und beschrieben, welche neuen Features darin zur Verfügung stehen, um VHD-Dateien zu erstellen, anzufügen, im Dateisystem bereitzustellen, zu trennen und zu löschen. Neben diesen neuen Features bietet die Datenträgerverwaltung auch die Möglichkeit, Basisdatenträger in dynamische Datenträger zu konvertieren (oder umgekehrt, was allerdings selten benötigt wird) und den Partitionsstil zu ändern. Windows 7 stellt für die Datenträgerverwaltung außerdem das Befehlszeilentool Diskpart zur Verfügung.



Hinweis Fdisk

Windows 7 unterstützt nicht mehr das Tool Fdisk, das in älteren Windows-Versionen für die Datenträgerverwaltung eingesetzt wurde.

Sie müssen zu den Gruppen *Administratoren* oder *Sicherungs-Operatoren* gehören, um die meisten Aufgaben im Bereich der Datenträgerverwaltung ausführen zu können. Sie können mit dem Tool Festplatten sowie die darin enthaltenen Volumes oder Partitionen verwalten. Sie können Datenträger initialisieren, Volumes anlegen und mit den Dateisystemen FAT, FAT32 oder NTFS formatieren. Sie können in der Datenträgerverwaltung diverse Operationen an Datenträgern ausführen, ohne das System neu starten zu müssen. Die meisten Konfigurationsänderungen werden sofort wirksam.

Arbeiten mit Partitionen

Sie können in der Datenträgerverwaltung Partitionen direkt in der grafischen Benutzeroberfläche vergrößern und verkleinern. Wenn Sie in der Konsole *Datenträgerverwaltung* mit der rechten Maustaste auf ein Volume klicken, bekommen Sie direkt im Kontextmenü die Möglichkeit angeboten, ein einfaches, übergreifendes oder Stripesetvolume zu erstellen. Fügen Sie mehr als vier Partitionen zu einem Basisdatenträger hinzu, werden Sie aufgefordert, den Datenträger in einen dynamischen zu konvertieren oder den GPT-Partitionsstil zu verwenden.

Sie können einen Datenträger in der Datenträgerverwaltung zwischen verschiedenen Typen und Partitionsstilen konvertieren. Einige Operationen lassen sich allerdings nicht mehr umkehren (sofern Sie das Laufwerk nicht neu partitionieren). Sie sollten sorgfältig überlegen, welcher Datenträgertyp und Partitionsstil sich am besten für Ihre Anwendung eignet. Es sind Konvertierungen zwischen folgenden Partitionsstilen möglich:

- MBR kann in GPT konvertiert werden, sofern sich noch keine Volumes auf dem Datenträger befinden.
- MBR kann in einen dynamischen Datenträger konvertiert werden, aber von diesem Datenträger kann unter Umständen nicht mehr gestartet werden.
- GPT kann in MBR konvertiert werden, sofern sich noch keine Volumes auf dem Datenträger befinden.
- GPT kann in einen dynamischen Datenträger konvertiert werden, aber von diesem Datenträger kann unter Umständen nicht mehr gestartet werden.
- Ein dynamischer Datenträger kann in MBR konvertiert werden, sofern sich noch keine Volumes auf dem Datenträger befinden.
- Ein dynamischer Datenträger kann in GPT konvertiert werden, sofern sich noch keine Volumes auf dem Datenträger befinden.

Wenn Sie einen neuen Datenträger zu einem Computer hinzufügen, wird er als *Nicht initialisiert* aufgelistet. Bevor Sie einen solchen Datenträger benutzen können, müssen Sie ihn initialisieren. Wenn Sie die Datenträgerverwaltung starten, nachdem Sie einen neuen Datenträger hinzugefügt haben, öffnet sich der Assistent *Datenträgerinitialisierung*. Sie können auch mit der rechten Maustaste auf einen nicht initialisierten Datenträger klicken und den Befehl *Datenträgerinitialisierung* wählen. In diesem Fall wird der Datenträger als Basisdatenträger initialisiert, und Sie können auswählen, ob Sie den Partitionsstil MBR oder GPT verwenden wollen.

GPT-Datenträger haben unter anderem den Vorteil, dass Sie mehr als vier Partitionen auf jedem Datenträger anlegen können. GPT wird auch gebraucht, wenn eine Festplatte größer ist als 2 TByte. Sie können bei einem Basisdatenträger den Partitionsstil von MBR auf GPT ändern, solange er noch keine Partitionen oder Volumes enthält. Befinden sich Daten auf dem MBR-Datenträger, müssen Sie erst eine Datensicherung ausführen und dann nach der Konvertierung eine Wiederherstellung.

Sie können in der Datenträgerverwaltung alle Volumes oder Partitionen von dem Datenträger löschen, den Sie konvertieren wollen, und dann die Konvertierung ausführen. Klicken Sie mit der rechten Maustaste nacheinander auf jedes Volume und wählen Sie den Befehl *Volume löschen*. Enthält der Datenträger keine Volumes oder Partitionen mehr, können Sie ihn mit der rechten Maustaste anklicken und den Befehl *Zu GPT-Datenträger konvertieren* wählen.



Hinweis Wechseldatenträger

Für Wechseldatenträger können Sie den Partitionsstil GPT nicht verwenden.

Gehen Sie folgendermaßen vor, um mit dem Befehlszeilenprogramm Diskpart den Partitionsstil eines Datenträgers von MBR auf GPT zu ändern:

1. Sichern Sie die Daten auf dem MBR-Basisdatenträger, den Sie konvertieren wollen.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben Sie **diskpart** ein.
3. Geben Sie an der DISKPART>-Eingabeaufforderung **list volume** ein. Notieren Sie sich die Volumenummern.
4. Geben Sie an der DISKPART>-Eingabeaufforderung für jedes aufgeführte Volume den Befehl **select volume <*Volumenummer*>** ein.
5. Geben Sie für jedes Volume an der DISKPART>-Eingabeaufforderung den Befehl **delete volume** ein.
6. Geben Sie an der DISKPART>-Eingabeaufforderung **list disk** ein. Merken Sie sich die Nummer des Datenträgers, den Sie konvertieren wollen.
7. Geben Sie an der DISKPART>-Eingabeaufforderung **select disk <*Datenträgernummer*>** ein.
8. Geben Sie an der DISKPART>-Eingabeaufforderung **convert gpt** ein.

Sie können sowohl die Datenträgerverwaltung als auch das Tool Diskpart verwenden, um einen GPT- in einen MBR-Datenträger zu konvertieren. Der Ablauf ist fast derselbe wie beim Konvertieren von MBR in GPT. Sie müssen zuerst alle Daten sichern und dann alle Volumes löschen. Klicken Sie dann in der Datenträgerverwaltung mit der rechten Maustaste auf den Datenträger und wählen Sie den Befehl *Zu MBR-Datenträger konvertieren*. Wenn Sie mit Diskpart arbeiten, lautet der entsprechende Befehl im letzten Schritt **convert mbr**.

Verwenden von Basis- und dynamischen Datenträgern

Basisdatenträger haben MBR-Partitionstabellen im herkömmlichen MS-DOS-Stil, in denen sie Informationen zu primären und logischen Festplattenpartitionen speichern. Dynamische Datenträger verwenden einen reservierten Bereich auf dem Datenträger, um eine LDM-Datenbank (Logical Disk Manager) zu speichern. Diese LDM-Datenbank enthält Typ, Offset, Mitgliedschaften und Laufwerkbuchstabe jedes Volumes. Die LDM-Datenbank wird auch repliziert, sodass jeder dynamische Datenträger die Konfiguration aller anderen dynamischen Datenträger kennt. Aufgrund dieses Features sind dynamische Datenträger wesentlich zuverlässiger und besser wiederherstellbar als Basisdatenträger.

Wenn Sie einen dynamischen Datenträger von einem Computer zum anderen verschieben, kann es allerdings vorkommen, dass Sie ihn anschließend nicht mehr auf den ursprünglichen Host zurückschieben können. Wenn Sie dynamische Datenträger verschieben, sollten Sie daher alle dynamischen Datenträger eines Computers zusammen verschieben und sicherstellen, dass sie alle online sind und auf dem Zielcomputer laufen, bevor Sie versuchen, sie zu importieren. Der Name der Datenträgergruppe und die Identität der primären Datenträgergruppe des Hostsystems werden immer beibehalten, wenn ein dynamischer Datenträger vorhanden ist. Gibt es auf dem Zielcomputer noch keine dynamischen Datenträger, erhält dieser Computer denselben Datenträgergruppennamen wie der Quellcomputer, wenn die Datenträ-

ger dorthin verschoben werden. In diesem Fall können Sie die Datenträger nicht zurück auf den Quellcomputer verschieben.

Microsoft empfiehlt, einen Basisdatenträger erst dann in einen dynamischen Datenträger zu konvertieren, wenn Sie überprüft haben, ob Sie tatsächlich die Features brauchen, die dynamische Datenträger bieten. Haben Sie nicht vor, diese Features zu nutzen, ist es am besten, Basisdatenträger zu verwenden. Um einen Basisdatenträger in einen dynamischen Datenträger zu konvertieren, können Sie entweder die Datenträgerverwaltung oder das Befehlszeilenprogramm Diskpart verwenden.



Vorsicht Konvertieren von Datenträgern

Bevor Sie Datenträger konvertieren, sollten Sie alle Programme schließen, die auf diesen Datenträgern laufen.

Schnelltest

- Bei welchem Partitionstyp können Sie mehr als vier Partitionen auf jedem Laufwerk anlegen?

Antwort zum Schnelltest

- GPT

Wenn Sie einen Basisdatenträger mithilfe der Datenträgerverwaltung in einen dynamischen Datenträger konvertieren wollen, müssen Sie mit der rechten Maustaste auf den Datenträger klicken und dann den Befehl *In dynamischen Datenträger konvertieren* wählen.

Wollen Sie einen Basisdatenträger mit Diskpart in einen dynamischen Datenträger konvertieren, müssen Sie erst den Datenträger auswählen, den Sie konvertieren wollen, und dann an der DISKPART>-Eingabeaufforderung den Befehl **convert dynamic** eingeben. Diese Schritte arbeiten Sie in den Übungen weiter unten in dieser Lektion durch.

Wurde ein dynamischer Datenträger konvertiert, enthält er keine Basisvolumes mehr. Wenn Sie einen Basisdatenträger in einen dynamischen Datenträger konvertieren, werden alle vorhandenen Partitionen oder logische Laufwerke, die auf dem Basisdatenträger vorhanden waren, auf dem dynamischen Datenträger zu einfachen Volumes. Und nachdem Sie einen Basisdatenträger in einen dynamischen Datenträger konvertiert haben, können Sie die dynamischen Volumes nicht in Partitionen zurückverwandeln. Stattdessen müssen Sie alle dynamischen Volumes auf dem Datenträger löschen und ihn dann zurück in einen Basisdatenträger konvertieren. Wollen Sie Ihre Daten behalten, müssen Sie sie zuerst sichern oder auf ein anderes Volume kopieren.

Ein dynamischer Datenträger wird nur selten in einen Basisdatenträger konvertiert. Bei diesem Vorgang können ernste Probleme auftreten (beispielsweise müssen Sie die Daten sichern und alle dynamischen Volumes löschen). Sie können entweder die Datenträgerverwaltung oder das Befehlszeilenprogramm Diskpart verwenden, um einen dynamischen Datenträger in einen Basisdatenträger zurückzukonvertieren.

Wenn Sie die Datenträgerverwaltung verwenden, müssen Sie erst alle Volumes auf dem Datenträger sichern, den Sie konvertieren wollen. Klicken Sie dann in der Datenträgerverwaltung mit der rechten Maustaste auf jedes Volume und wählen Sie jeweils den Befehl

Volume löschen. Sind alle Volumes auf dem Datenträger gelöscht, können Sie mit der rechten Maustaste auf den Datenträger klicken und den Befehl *In einen Basisdatenträger konvertieren* wählen. Ein dynamischer Datenträger darf keine Volumes enthalten und es dürfen keine Daten darauf gespeichert sein, wenn Sie ihn in einen Basisdatenträger zurückkonvertieren wollen. Abbildung 4.35 zeigt das Kontextmenü eines Datenträgers in der Datenträgerverwaltung, mit dessen Befehlen Sie einen MBR- in einen GPT-Datenträger und einen Basisdatenträger in einen dynamischen Datenträger konvertieren.

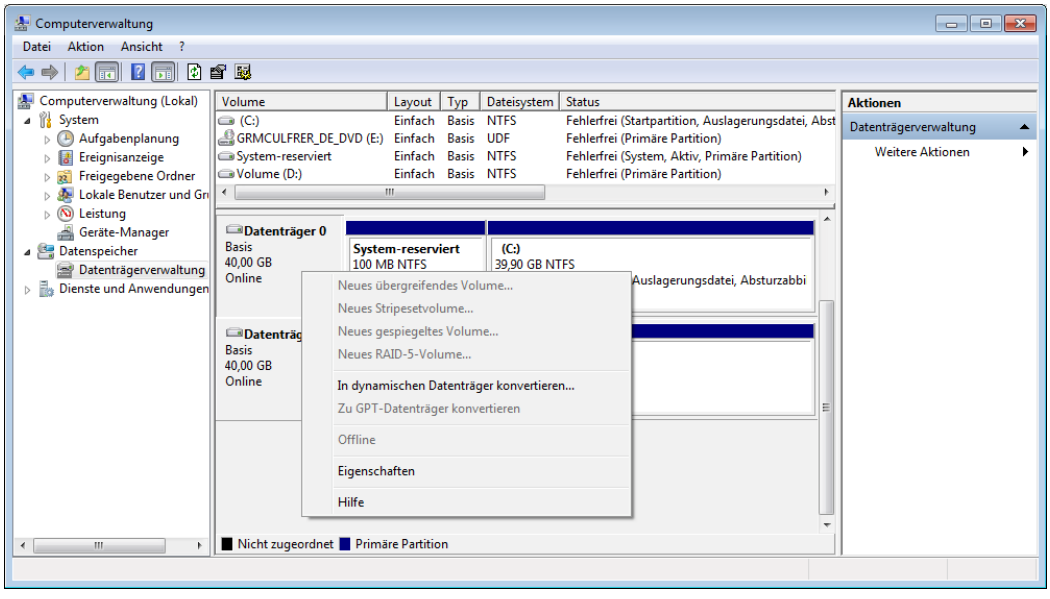


Abbildung 4.35 Kontextmenübefehle zum Konvertieren von MBR- und Basisdatenträgern

Gehen Sie folgendermaßen vor, um einen dynamischen Datenträger mit dem Tool Diskpart zurück in einen Basisdatenträger zu konvertieren:

1. Führen Sie eine Datensicherung aller Volumes auf dem Datenträger durch, den Sie konvertieren wollen.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben Sie **diskpart** ein.
3. Geben Sie an der DISKPART>-Eingabeaufforderung **list disk** ein. Notieren Sie sich die Nummer des Datenträgers, den Sie konvertieren wollen.
4. Geben Sie an der DISKPART>-Eingabeaufforderung **select disk <*Datenträgernummer*>** ein.
5. Geben Sie an der DISKPART>-Eingabeaufforderung **detail disk <*Datenträgernummer*>** ein.
6. Geben Sie für jedes Volume des Datenträgers an der DISKPART>-Eingabeaufforderung **select volume <*Volumenummmer*>** und dann **delete volume** ein.
7. Geben Sie an der DISKPART>-Eingabeaufforderung **select disk <*Datenträgernummer*>** ein.
8. Geben Sie an der DISKPART>-Eingabeaufforderung **convert basic** ein.

Umbauen von Datenträgern in andere Computer

Bevor Sie Datenträger in einen anderen Computer verschieben, sollten Sie in der Datenträgerverwaltung sicherstellen, dass der Status aller Volumes auf dem Datenträger als »Fehlerfrei« angezeigt wird. Ist der Status nicht fehlerfrei, sollten Sie die Volumes reparieren, bevor Sie den Datenträger verschieben. Sie überprüfen den Volumestatus, indem Sie in der Konsole *Datenträgerverwaltung* auf die Spalte *Status* klicken.

Im nächsten Schritt deinstallieren Sie den Datenträger, den Sie verschieben wollen. Öffnen Sie im Navigationsbereich der Computerverwaltung (im linken Fensterabschnitt) den Geräte-Manager. Klicken Sie in der Liste der Geräte doppelt auf *Laufwerke*. Klicken Sie nacheinander mit der rechten Maustaste auf jeden Datenträger, den Sie deinstallieren wollen, und wählen Sie den Befehl *Deinstallieren*. Klicken Sie im Dialogfeld *Deinstallation des Geräts bestätigen* auf *OK*.

Wenn die Datenträger, die Sie verschieben wollen, dynamische Datenträger sind, müssen Sie in der Datenträgerverwaltung mit der rechten Maustaste auf die Datenträger klicken und den Befehl *Datenträger löschen* wählen.

Nachdem Sie dynamische Datenträger gelöscht haben oder wenn Sie Basisdatenträger verschieben, können Sie die Festplattenlaufwerke aus dem Computer ausbauen. Handelt es sich um externe Geräte, brauchen Sie sie nur vom Computer abzustecken. Sind es interne Laufwerke, müssen Sie den Computer ausschalten und die Laufwerke dann abstecken und ausbauen.

Wenn Sie externe Datenträger verwenden, können Sie sie einfach an den Zielcomputer anstecken. Sind es interne Laufwerke, müssen Sie den Computer ausschalten und dann die Laufwerke einbauen. Starten Sie den Zielcomputer wieder und folgen Sie den Anweisungen im Dialogfeld *Neue Hardware gefunden*.

Öffnen Sie auf dem Zielcomputer die Datenträgerverwaltung und wählen Sie im Menü *Aktion* den Befehl *Datenträger neu einlesen*. Klicken Sie mit der rechten Maustaste auf alle Datenträger, die als *Fremd* markiert sind, wählen Sie den Befehl *Fremde Datenträger importieren* und folgen Sie dann den Anweisungen.

Wenn Sie Basisvolumes auf einen anderen Computer verschieben, bekommen sie den nächsten freien Laufwerkbuchstaben auf diesem Computer zugewiesen. Dynamische Volumes behalten den Laufwerkbuchstaben, den sie auf dem vorherigen Computer hatten. Falls ein dynamisches Volume auf dem vorherigen Computer keinen Laufwerkbuchstaben hatte, bekommt er auch keinen Laufwerkbuchstaben, wenn es in den neuen Computer verschoben wird. Wird der Laufwerkbuchstabe bereits auf dem neuen Computer benutzt, erhält ein Volume den nächsten freien Laufwerkbuchstaben. Wenn ein Administrator die Befehle `mountvol /n` oder `diskpart automount` ausgeführt hat, um zu verhindern, dass neue Volumes zum System hinzugefügt werden, werden Volumes, die von einem anderen Computer verschoben werden, nicht eingebunden und bekommen keinen Laufwerkbuchstaben zugewiesen. Um ein solches Volume benutzen zu können, müssen Sie es von Hand einbinden und ihm einen Laufwerkbuchstaben zuweisen. Dafür können Sie die Datenträgerverwaltung oder die Befehle `diskpart` und `mountvol` verwenden.

Wenn Sie übergreifende, Stripeset-, gespiegelte oder RAID-5-Volumes verschieben, müssen Sie alle Datenträger verschieben, die Teile des Volumes enthalten. Andernfalls können die Volumes auf den Datenträgern nicht online gebracht werden und sind nicht verfügbar. Sie müssen sie dann löschen.

Sie können mehrere Datenträger aus unterschiedlichen Computern in denselben Zielcomputer verschieben, indem Sie die Laufwerke einbauen, die Datenträgerverwaltung öffnen, mit der rechten Maustaste auf einen der neuen Datenträger klicken und den Befehl *Fremde Datenträger importieren* wählen. Wenn Sie mehrere Datenträger aus unterschiedlichen Computern importieren, müssen Sie immer alle Datenträger, die aus einem Quellcomputer stammen, zusammen importieren.

Die Datenträgerverwaltung zeigt den Status der Volumes auf einem Datenträger an, bevor sie importiert werden. Prüfen Sie diese Informationen sorgfältig, weil daraus oft hervorgeht, was mit jedem Volume passiert, sobald der Datenträger importiert wurde.

Reaktivieren eines fehlenden oder offline geschalteten dynamischen Datenträgers

Ein dynamischer Datenträger kann den Status »Fehlend« einnehmen, wenn er beschädigt ist, ausgeschaltet wurde oder das Kabel abgezogen wurde. Den Status »Offline« bekommt er, wenn er beschädigt oder vorübergehend nicht verfügbar ist, oder wenn Sie versuchen, einen fremden (dynamischen) Datenträger zu importieren und dies fehlschlägt. Ist ein Datenträger offline, wird er mit einem Fehlersymbol markiert. Nur dynamische Datenträger zeigen den Status »Fehlend« oder »Offline« an und können reaktiviert werden. Sie reaktivieren einen dynamischen Datenträger, indem Sie ihn in der Datenträgerverwaltung mit der rechten Maustaste anklicken und den Befehl *Datenträger reaktivieren* wählen.

Sie können dafür auch das Tool Diskpart verwenden. Wie in den vorherigen Anleitungen listen Sie dabei die Datenträger auf und notieren sich die Nummer des Datenträgers, den Sie reaktivieren wollen. Dann wählen Sie den Datenträger anhand seiner Nummer aus und geben an der DISKPART>-Eingabeaufforderung den Befehl `online` ein.

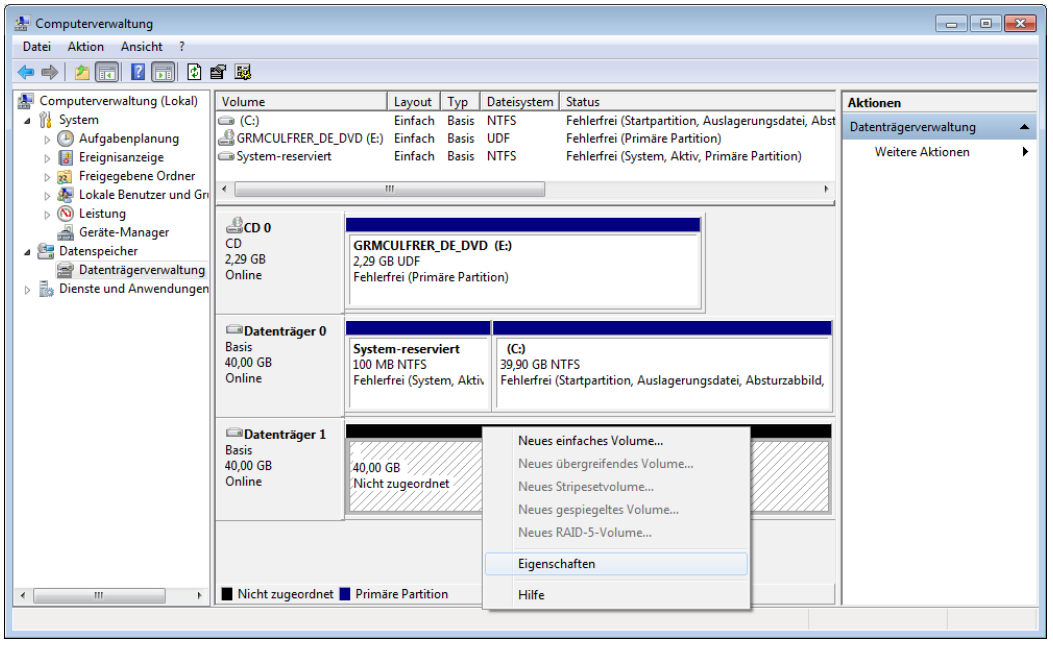


Abbildung 4.36 Befehle zum Anlegen von Volumes

Stattdessen können Sie einen fehlenden dynamischen Datenträger auch löschen. Löschen Sie dazu erst alle Volumes auf dem fehlenden Datenträger, entweder in der Datenträgerverwaltung oder im Tool Diskpart. In der Datenträgerverwaltung müssen Sie mit der rechten Maustaste auf den Datenträger klicken und den Befehl *Löschen* wählen. Wenn Sie Diskpart verwenden, lassen Sie sich die Datenträger auflisten, notieren sich die Datenträgernummer, wählen den Datenträger anhand seiner Nummer aus und geben an der DISKPART>-Eingabeaufforderung den Befehl `delete disk` ein.

Verwalten von Datenträgervolumes

Sie können Volumes in Windows 7 ohne Datenverlust vergrößern und verkleinern, es ist nicht einmal ein Neustart notwendig. Sie können auf dynamischen Datenträgern einfache Volumes, übergreifende Volumes, Stripesetvolumes, gespiegelte Volumes und Stripesetvolumes mit Parity anlegen. Auf Basisdatenträgern können Sie einfache Volumes erstellen. Abbildung 4.36 zeigt, welche Befehle zur Verfügung stehen, um Volumes auf nicht zugewiesenen Bereichen eines Datenträgers anzulegen.

Erstellen eines einfachen Volumes

In Windows 7 (und Windows Vista) können einfache Volumes sowohl Partitionen auf Basisdatenträgern als auch einfache Volumes auf dynamischen Datenträgern umfassen. Werden alle Ihre Anforderungen von einem einfachen Volume erfüllt, empfiehlt Microsoft, einen Basisdatenträger zu verwenden.

Gehen Sie folgendermaßen vor, um in der Datenträgerverwaltung ein einfaches Volume anzulegen:

1. Öffnen Sie die Datenträgerverwaltung.
2. Klicken Sie mit der rechten Maustaste auf einen nicht zugewiesenen Bereich in Ihrem Datenträger und wählen Sie den Befehl *Neues einfaches Volume*. Daraufhin wird der Assistent zum Erstellen neuer einfacher Volumes gestartet.
3. Geben Sie auf der Seite *Volumegröße festlegen* die Größe des Volumes, das Sie anlegen wollen, in der Einheit MByte ein. Standardeinstellung ist der gesamte freie Platz auf dem Datenträger.
4. Wählen Sie auf der Seite *Laufwerkbuchstaben oder -pfad zuordnen* einen Laufwerkbuchstaben oder einen Bereitstellungspunkt aus.
5. Wählen Sie auf der Seite *Partition formatieren* die Formatierungsoptionen aus.
6. Lesen Sie auf der Seite *Fertigstellen des Assistenten* die Zusammenfassung der gewählten Einstellungen. Klicken Sie auf *Fertig stellen*, wenn alles richtig ist.

Auf diese Weise erstellen Sie einfache Volumes auf dynamischen Datenträgern sowie primäre Partitionen auf GPT-Basisdatenträgern. Bei MBR-Basisdatenträgern sind die ersten drei Volumes, die Sie erstellen, primäre Partitionen. Das vierte einfache Volume auf einem MBR-Basisdatenträger wird dagegen als erweiterte Partition mit einem logischen Laufwerk erstellt. Alle weiteren einfachen Volumes auf dem MBR-Basisdatenträger sind dann logische Laufwerke.

Wenn Sie ein einfaches Volume mit dem Tool Diskpart erstellen, müssen Sie unterscheiden, ob der Datenträger, auf dem Sie das Volume erstellen wollen, ein dynamischer oder ein Basisdatenträger ist. In Diskpart erstellen Sie auf einem Basisdatenträger eine Partition, auf einem dynamischen Datenträger dagegen ein Volume. Sie erstellen ein einfaches Volume auf

einem dynamischen Datenträger, indem Sie an der DISKPART>-Eingabeaufforderung einen Befehl mit folgender Syntax eingeben:

```
create volume simple [size=<n>] [disk=<n>]
```

Erstellen eines übergreifenden Volumes

Ein übergreifendes Volume (spanned volume) nutzt freien Platz auf mehreren physischen Festplatten, um ein Volume zu bilden. Die Abschnitte, die auf den unterschiedlichen Datenträgern für das Volume verwendet werden, brauchen nicht gleich groß zu sein. Außerdem dürfen sich mehrere Abschnitte des Volumes auf demselben Datenträger befinden. Ein übergreifendes Volume erhöht die Gefahr eines Ausfalls, der zu Datenverlust führt. Fällt auch nur ein einziges Laufwerk aus, das am übergreifenden Volume beteiligt ist, wird das gesamte Volume unbrauchbar.

Übergreifende Volumes bieten keinen deutlichen Leistungsvorteil. Wenn Sie die Geschwindigkeit durch Einsatz mehrerer Laufwerke erhöhen wollen, müssen Sie Stripesets nutzen, wie sie beispielsweise RAID-Arrays verwenden (etwa RAID-0 oder RAID-5). Der Vorteil eines übergreifenden Volumes liegt darin, dass die verwendeten Abschnitte auf jedem Datenträger unterschiedlich groß sein dürfen und mehrere Abschnitte auf demselben Laufwerk liegen dürfen. RAID-Arrays werden weiter unten in dieser Lektion behandelt.

Gehen Sie folgendermaßen vor, um in der Datenträgerverwaltung ein übergreifendes Volume zu erstellen:

1. Öffnen Sie die Datenträgerverwaltung.
2. Klicken Sie mit der rechten Maustaste auf einen nicht zugeordneten Bereich, den Sie in das übergreifende Volume aufnehmen wollen, und wählen Sie im Kontextmenü den Befehl *Neues übergreifendes Volume*. Der Assistent *Neues übergreifendes Volume* wird gestartet.
3. Wählen Sie auf der Seite *Datenträger auswählen* alle Datenträger aus, die Sie verwenden wollen, und klicken Sie auf *Hinzufügen*, um sie zum übergreifenden Volume hinzuzufügen. Wählen Sie jeden Datenträger im Listenfeld *Ausgewählt* aus und stellen Sie ein, wie viel Platz auf diesem Datenträger für das übergreifende Volume benutzt werden soll.
4. Auf der Seite *Laufwerkbuchstaben oder -pfad zuordnen* wird dem neuen Volume als Standardeinstellung der nächste freie Laufwerkbuchstabe zugewiesen. Sie können das Volume auch in einem leeren NTFS-Ordner auf einem vorhandenen Volume bereitstellen.
5. Wählen Sie auf der Seite *Volume formatieren* die Formatierungsoptionen für das neue Volume aus. Windows 7 unterstützt im Snap-In *Datenträgerverwaltung* nur die Formatierung mit NTFS. Wenn Sie das Volume mit FAT oder FAT32 formatieren wollen, müssen Sie das Tool Diskpart verwenden.
6. Lesen Sie auf der Seite *Fertigstellen des Assistenten* die Zusammenfassung der gewählten Einstellungen. Klicken Sie auf *Fertig stellen*, wenn alles richtig ist.

Wenn Sie mit Diskpart ein übergreifendes Volume erstellen wollen, müssen Sie sicherstellen, dass die verwendeten Datenträger in dynamische Datenträger konvertiert werden. Dann legen Sie ein einfaches Volume auf dem ersten Datenträger des übergreifenden Volumes an, erweitern das Volume auf den zweiten Datenträger und fügen alle weiteren Datenträger hinzu,

die an dem übergreifenden Volume beteiligt sein sollen. Schließlich weisen Sie dem Volume einen Laufwerkbuchstaben oder einen Bereitstellungspunkt zu.

Auf welche Weise Sie mit Diskpart ein übergreifendes Volume erstellen, hängt davon ab, ob der ausgewählte Datenträger ein Basis- oder ein dynamischer Datenträger ist. Auf einem Basisdatenträger können Sie ein übergreifendes Volume nur anlegen, wenn genug Platz für das gesamte ausgewählte Volume in einem zusammenhängenden Abschnitt frei ist. Dann geben Sie einen Befehl mit der Syntax `extend [size=<n>]` ein. Wenn Sie das Argument mit der Größenangabe weglassen, nimmt das übergreifende Volume den gesamten freien Platz ein. Verwenden Sie dagegen einen dynamischen Datenträger mit einem einfachen oder übergreifenden Volume, können Sie das Volume auf einen zweiten Datenträger ausweiten, auf dem noch Platz frei ist. Nachdem Sie ein Volume ausgewählt haben, führen Sie einen Befehl mit der Syntax `extend [size=<n>] [disk=<n>]` aus. Wenn Sie das Argument `disk` weglassen, wird das übergreifende Volume auf demslben Datenträger erstellt wie das ausgewählte Volume. Lassen Sie das Argument `size` weg, nimmt das übergreifende Volume den gesamten nicht zugewiesenen Platz ein.

Erstellen eines Stripesetvolumes (RAID-0)

Ein Stripesetvolume verwendet Platz auf mehreren physischen Festplatten, um ein Volume zu bilden. Das Betriebssystem schreibt dabei kleine Blöcke (die sogenannten stripes, dt. »Streifen«) auf die Datenträger, sodass sich die Last über alle Datenträger des Volumes verteilt. Daten werden in einen Block auf dem ersten Laufwerk geschrieben, dann in einen Block auf dem zweiten Laufwerk und so weiter. Die Daten werden dabei in Blöcke aufgeteilt, die genauso groß sind wie ein Stripe, und auf alle Laufwerke gleichzeitig geschrieben. Ein Stripesetvolume (RAID-0) muss mindestens zwei Datenträger umfassen.

Werden Daten aus dem Volume gelesen, kann parallel auf alle Laufwerke zugegriffen werden, die am Volume beteiligt sind. RAID-0 verbessert daher sowohl die Lese- als auch die Schreibgeschwindigkeit ganz erheblich. Die Abschnitte, die für das Volume benutzt werden, müssen auf allen Datenträgern gleich groß sein. Es hängt daher von dem Datenträger mit dem wenigsten freien Platz ab, wie groß das Stripesetvolume höchstens werden kann. Ein Stripesetvolume bietet keine Fehlertoleranz. Ist ein einziges Laufwerk defekt, fällt das gesamte Volume aus.

Gehen Sie folgendermaßen vor, um in der Datenträgerverwaltung ein Stripesetvolume zu erstellen:

1. Öffnen Sie die Datenträgerverwaltung.
2. Klicken Sie mit der rechten Maustaste auf einen nicht zugeordneten Bereich, den Sie in das Stripesetvolume aufnehmen wollen, und wählen Sie im Kontextmenü den Befehl *Neues Stripesetvolume*. Der Assistent *Neues Stripesetvolume* wird gestartet.
3. Wählen Sie auf der Seite *Datenträger auswählen* alle Datenträger aus, die Sie verwenden wollen, und klicken Sie auf *Hinzufügen*, um sie zum Stripesetvolume hinzuzufügen. Wählen Sie aus, wie viel Platz Sie auf jedem Datenträger für das Stripesetvolume benutzen wollen.
4. Auf der Seite *Laufwerkbuchstaben oder -pfad zuordnen* wird dem neuen Volume als Standardeinstellung der nächste freie Laufwerkbuchstabe zugewiesen. Sie können das Volume auch in einem leeren NTFS-Ordner auf einem vorhandenen Volume bereitstellen.

5. Wählen Sie auf der Seite *Volume formatieren* die Formatierungsoptionen für das neue Stripesetvolume aus. Windows 7 unterstützt im Snap-In *Datenträgerverwaltung* nur die Formatierung mit NTFS. Wenn Sie das Volume mit FAT oder FAT32 formatieren wollen, müssen Sie das Tool Diskpart verwenden.
6. Lesen Sie auf der Seite *Fertigstellen des Assistenten* die Zusammenfassung der gewählten Einstellungen. Klicken Sie auf *Fertig stellen*, wenn alles richtig ist.

Um mit Diskpart ein Stripesetvolume auf einem dynamischen Datenträger zu erstellen, geben Sie einen Befehl mit folgender Syntax an die DISKPART>-Eingabeaufforderung ein:

```
create volume stripe [size=<n>] disk=<n>[,<n>[,..]]
```

Die Gesamtgröße des Stripesetvolumes ergibt sich aus dem Produkt der angegebenen Größe und der Zahl der Datenträger.

Erstellen eines gespiegelten Volumes (RAID-1)

Ein gespiegeltes oder RAID-1-Volume (mirrored volume) bietet hohe Verfügbarkeit und Fehlertoleranz, verbessert aber nicht die Leistung. Es verwendet zwei Datenträger (oder zwei Abschnitte auf unterschiedlichen Datenträgern), die gleich groß sind. Jede Änderung, die am ersten Datenträger eines Spiegelsatzes vorgenommen wird, wird auch in den gespiegelten Datenträger geschrieben. Fällt der erste Datenträger aus, ist der Spiegel »zerbrochen«, aber der zweite Datenträger kann benutzt werden, bis der erste repariert oder ausgetauscht ist. Anschließend wird der Spiegel neu erstellt, wobei die Daten des funktionierenden Datenträgers auf den reparierten Datenträger kopiert werden. RAID-1 hat den Nachteil, dass Sie (beispielsweise) zwei 200-GByte-Festplatten brauchen, um insgesamt 200 GByte Daten zu speichern. Der Vorteil ist, dass Sie einen Systemdatenträger spiegeln können, der Ihr Betriebssystem enthält.

Um ein gespiegeltes Volume zu erstellen, gehen Sie ganz ähnlich vor wie bei einem Stripesetvolume, allerdings klicken Sie mit der rechten Maustaste auf den ersten Datenträger des Spiegels und wählen den Befehl *Neues gespiegeltes Volume*, um den gleichnamigen Assistenten zu starten. Dann wählen Sie den zweiten Datenträger aus. Der zweite Datenträger muss einen nicht zugewiesenen Abschnitt haben, der mindestens genauso groß ist wie der Datenträger, den Sie spiegeln wollen. Der Laufwerkbuchstabe für ein gespiegeltes Volume ist derselbe wie der für den ersten Datenträger.

Sie können auch das Tool Diskpart verwenden, um ein gespiegeltes Volume zu erstellen. Wählen Sie an der DISKPART>-Eingabeaufforderung zuerst mit `select disk` den ersten Datenträger aus. Geben Sie dann einen Befehl mit der Syntax `add disk=<n>` ein, um den Spiegeldatenträger anzugeben.

Erstellen eines Stripesetvolumes mit Parity (RAID-5)

Ein Stripesetvolume mit Parity bietet Hochverfügbarkeit, Ausfallschutz und Leistungssteigerung. Sie brauchen dafür mindestens drei Laufwerke oder gleichgroße Abschnitte mit freiem Platz auf mindestens drei unterschiedlichen Datenträgern. Das Volume ist ähnlich wie bei RAID-0 in »Streifen« unterteilt, aber hier wird auf jedem Datenträger ein Teil der Kapazität genutzt, um Paritydaten zu speichern. Das sind komprimierte Informationen über den Inhalt der anderen Datenträger im Satz.

Fällt ein Datenträger aus, liegen seine Daten noch auf den anderen Datenträgern im Satz vor. Der Zugriff ist in diesem Fall allerdings langsamer, weil die Paritydaten dekomprimiert wer-

den müssen. Wird ein Ersatzlaufwerk eingebaut, kann sein Inhalt anhand der Paritydaten aus den anderen Datenträgern wiederhergestellt werden.

Die Leseleistung ist bei RAID-5 besser (sofern alle Datenträger funktionieren), weil Daten von allen Datenträgern im Satz parallel gelesen werden können. Zwar können auch Daten parallel auf alle Datenträger geschrieben werden, aber andererseits müssen bei jeder Schreiboperation zusätzliche Paritydaten berechnet und geschrieben werden. RAID-5 bietet daher eine Verbesserung bei der Schreibleistung, sie ist aber nicht so deutlich wie die Steigerung bei der Leseleistung.

Paritydaten verbrauchen genau so viel Festplattenplatz, wie ein Datenträger des RAID-5-Satzes speichert. Wenn Sie also drei Datenträger mit jeweils 200 GByte Größe haben, erhalten Sie eine nutzbare Kapazität von 400 GByte. Haben Sie vier Datenträger mit jeweils 200 GByte, beträgt die nutzbare Kapazität 600 GByte, und so weiter.

Ein RAID-5-Volume kann keine Systeminformationen enthalten und nicht Ihr Betriebssystem speichern. Üblicherweise setzen Sie RAID-5 zum Speichern von Daten ein, weil es Ausfallschutz und bessere Leistung bietet. Mit RAID-1 spiegeln Sie Ihr Betriebssystem, damit Sie den Computer auch dann noch starten können, wenn eine Festplatte ausfällt. Sie können RAID-0 für die Datenspeicherung einsetzen, wenn Sie optimale Lese- und Schreibleistung brauchen, aber Sie müssen sich in diesem Fall bewusst sein, dass RAID-0 keinerlei Fehlertoleranz bietet.



Hinweis Hardware-RAID

Windows 7 stellt Softwareimplementierungen von RAID-0, RAID-1 und RAID-5 bereit, die keine zusätzliche Hardware benötigen. Sie können auch Hardware-RAID-Systeme kaufen, die bestimmte Vorteile bieten (aber auch ihren Preis haben). Beispielsweise können einige Hardware-RAID-5-Systeme Systemdateien speichern. Sie können auch andere RAID-Systeme kaufen. RAID-10 implementiert zum Beispiel zwei Sätze mit Stripesetvolumes (RAID-0), die dann gespiegelt werden (RAID-1). Das bietet sowohl deutliche Leistungssteigerung als auch Ausfallschutz.



Prüfungstipp

In der Prüfung 70-680 bekommen Sie wahrscheinlich Fragen zur Softwareimplementierung von RAID in Windows 7. Es ist unwahrscheinlich, dass Sie etwas über Hardware-RAID-Systeme anderer Hersteller wissen müssen.

Sie erstellen ein Stripesetvolume mit Parity ganz ähnlich wie ein Stripesetvolume. Klicken Sie mit der rechten Maustaste auf den ersten Datenträger mit nicht zugewiesenem Platz und wählen Sie im Kontextmenü den Befehl *Neues RAID-5-Volume*, um den gleichnamigen Assistenten zu starten. Wählen Sie dann die anderen Datenträger für den Satz aus und legen Sie die Größe des Volumes fest. In der Standardeinstellung wird auf allen Datenträgern so viel Platz verwendet, wie auf dem Datenträger mit dem wenigsten freien Platz verfügbar ist. Ein Beispiel: Wenn auf dem ersten ausgewählten Datenträger 100 GByte nicht zugewiesen sind, auf dem zweiten 150 GByte und auf dem dritten 200 GByte, wird standardmäßig ein 300 GByte großes RAID-5-Volume erstellt, das eine Nutzkapazität von 200 GByte hat.

Wie bei einem RAID-0-Volume geben Sie anschließend den Laufwerkbuchstaben oder Bereitstellungspunkt und die Formatierungsoptionen an.

Sie können ein RAID-5-Volume auch mit dem Tool Diskpart erstellen. Geben Sie dazu an der DISKPART>-Eingabeaufforderung einen Befehl mit der folgenden Syntax ein:

```
create volume raid [size=<n>] disk=<n>[,<n>[,..]]
```

Ändern der Volumegröße

Sie können einfache Volumes und übergreifende Volumes in Windows 7 vergrößern und verkleinern. Die Größe von Stripesetvolumes ist allerdings fest. Wollen Sie bei einem Stripesetvolume die Größe ändern, müssen Sie es löschen und neu erstellen.

Gehen Sie folgendermaßen vor, um ein Volume in der Datenträgerverwaltung zu verkleinern:

1. Öffnen Sie die Konsole *Datenträgerverwaltung*.
2. Klicken Sie mit der rechten Maustaste auf das Volume, das Sie verkleinern wollen, und wählen Sie den Befehl *Volume verkleinern*. Die Datenträgerverwaltung untersucht das Volume, um festzustellen, wie viel Platz höchstens freigegeben werden kann. Das kann einige Zeit dauern.
3. Das Dialogfeld *Verkleinern* (Abbildung 4.37) zeigt, wie weit Sie das Volume höchstens verkleinern können (in der Einheit MByte). Stellen Sie ein, wie weit Sie das Volume verkleinern wollen, und klicken Sie auf *Verkleinern*. Daraufhin wird das Volume ohne weitere Nachfragen verkleinert.

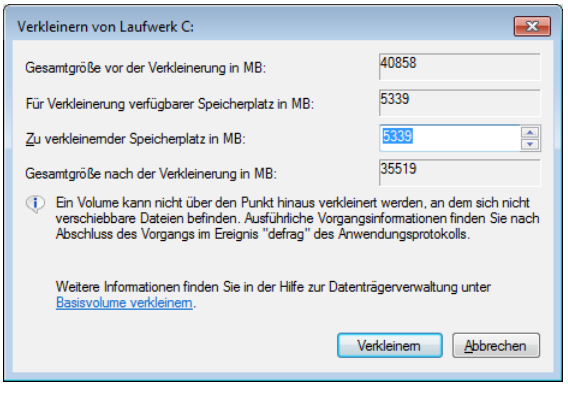

Verkleinern von Laufwerk C:
Gesamtgröße vor der Verkleinerung in MB:
40858
Für Verkleinerung verfügbarer Speicherplatz in MB:
5339
Zu verkleinemder Speicherplatz in MB:
5339
Gesamtgröße nach der Verkleinerung in MB:
35519
Ein Volume kann nicht über den Punkt hinaus verkleinert werden, an dem sich nicht verschiebbare Dateien befinden. Ausführliche Vorgangsinformationen finden Sie nach Abschluss des Vorgangs im Ereignis "defrag" des Anwendungsprotokolls.
Weitere Informationen finden Sie in der Hilfe zur Datenträgerverwaltung unter Basisvolume verkleinern.
Verkleinern
Abbrechen

Abbildung 4.37 Das Dialogfeld zum Verkleinern eines Volumes

Sie können auch das Tool Diskpart verwenden, um alle Volumes aufzulisten, die verkleinert werden können, und ein ausgewähltes Volume zu verkleinern. Gehen Sie dabei folgendermaßen vor:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **diskpart** ein.
3. Geben Sie an der DISKPART>-Eingabeaufforderung **list volume** ein.
4. Wählen Sie das Volume aus, das Sie verkleinern wollen. Geben Sie zum Beispiel **select volume 2** ein.
5. Stellen Sie fest, wie weit das Volume höchstens verkleinert werden kann, indem Sie **shrink querymax** eingeben.

6. Verkleinern Sie das ausgewählte Volume, indem Sie einen Befehl der Form **shrink desired=<*n*>** eingeben, wobei *<n>* in MByte angibt, um welche Größe das Volume verkleinert wird. Abbildung 4.38 zeigt den gesamten Ablauf.

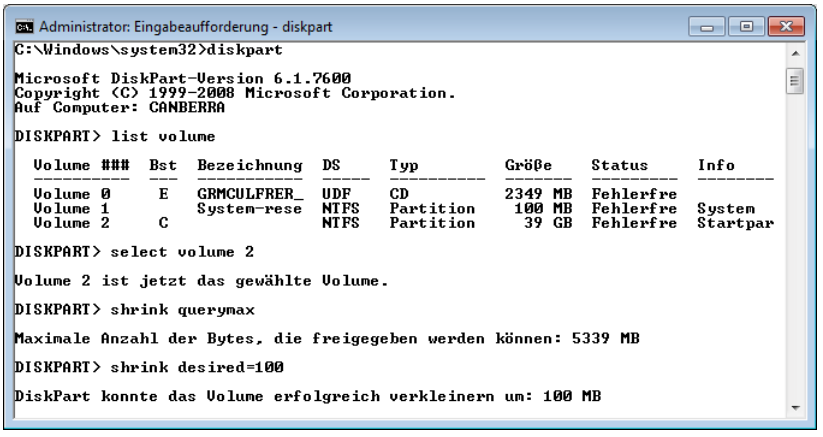

Administrator: Eingabeaufforderung - diskpart
C:\Windows\system32>diskpart
Microsoft DiskPart-Version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
Auf Computer: CANBERRA
DISKPART> list volume
Volume ### Bst Bezeichnung DS Typ Größe Status Info
Volume 0 E GRMCULFRER_ UDF CD 2349 MB Fehlerfre
Volume 1 System-rese NTFS Partition 100 MB Fehlerfre System
Volume 2 C NTFS Partition 39 GB Fehlerfre Startpar
DISKPART> select volume 2
Volume 2 ist jetzt das gewählte Volume.
DISKPART> shrink querymax
Maximale Anzahl der Bytes, die freigegeben werden können: 5339 MB
DISKPART> shrink desired=100
DiskPart konnte das Volume erfolgreich verkleinern um: 100 MB

Abbildung 4.38 Verkleinern eines Volumes mit Diskpart

Um ein Volume zu vergrößern, gehen Sie ganz ähnlich vor. In der Datenträgerverwaltung klicken Sie mit der rechten Maustaste auf das Volume, das Sie vergrößern wollen, wählen den Befehl *Volume erweitern* und gehen den Assistenten durch. Wenn Sie Diskpart verwenden, müssen Sie ein Volume auswählen und dann einen Befehl mit folgender Syntax eingeben:

```
extend [size=<n>] [disk=<n>]
```

Löschen eines Volumes

Sie können ein Volume entweder im Snap-In *Datenträgerverwaltung* oder auf einer Befehlszeile löschen. Wenn Sie ein Volume löschen, werden alle Daten, die darauf gespeichert sind, für immer gelöscht.

Klicken Sie in der Konsole *Datenträgerverwaltung* mit der rechten Maustaste auf das Volume und wählen Sie den Befehl *Volume löschen*. In der DISKPART>-Eingabeaufforderung listen Sie die Volumes mit dem Befehl `list volume` auf, wählen das gewünschte Volume aus (zum Beispiel mit `select volume 3`) und geben schließlich den Befehl `delete volume` ein.

Schnelltest

- Sie haben im Tool Diskpart ein Volume ausgewählt. Welcher Befehl verrät Ihnen, wie weit Sie das Volume höchstens verkleinern können?

Antwort zum Schnelltest

- `shrink querymax`



Weitere Informationen Diskpart

Weitere Informationen über das Befehlszeilentool Diskpart finden Sie unter *http://support.microsoft.com/kb/300415*.

Übung Konfigurieren von Zugriffsrichtlinien und Konvertieren eines Datenträgers

In dieser Übung konfigurieren Sie im Editor für lokale Gruppenrichtlinien eine Computerrichtlinie, die den Schreibzugriff auf USB-Flashsticks verbietet. Dann konvertieren Sie im Befehlszeilenprogramm Diskpart einen Basisdatenträger in einen dynamischen Datenträger.

Übung 1 Konfigurieren des Schreibzugriffs auf USB-Flashspeichergeräte

In dieser Übung deaktivieren Sie den Schreibzugriff auf USB-Flashstickgeräte. Dann löschen Sie diese Konfigurationseinstellung wieder.

1. Stecken Sie einen USB-Flashstick an Ihren Computer an.
2. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
3. Geben Sie im Suchfeld des Startmenüs **gpedit.msc** ein. Daraufhin öffnet sich der Editor für lokale Gruppenrichtlinien.
4. Erweitern Sie im linken Fensterabschnitt des Editors für lokale Gruppenrichtlinien die Zweige *Computerkonfiguration* und dann *Administrative Vorlagen*.
5. Erweitern Sie den Zweig *System* und klicken Sie auf *Wechselmedienzugriff*.

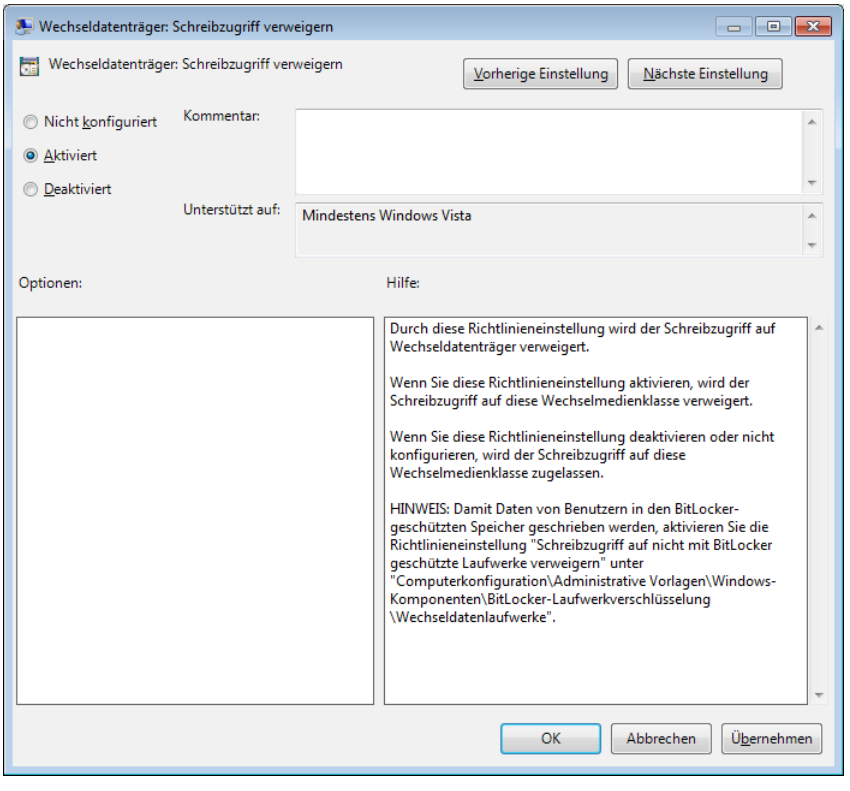

Wechseldatenträger: Schreibzugriff verweigern
Wechseldatenträger: Schreibzugriff verweigern
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows Vista
Optionen:
Hilfe:
Durch diese Richtlinieneinstellung wird der Schreibzugriff auf Wechseldatenträger verweigert.
Wenn Sie diese Richtlinieneinstellung aktivieren, wird der Schreibzugriff auf diese Wechselmedienklasse verweigert.
Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird der Schreibzugriff auf diese Wechselmedienklasse zugelassen.
HINWEIS: Damit Daten von Benutzern in den BitLocker-geschützten Speicher geschrieben werden, aktivieren Sie die Richtlinieneinstellung "Schreibzugriff auf nicht mit BitLocker geschützte Laufwerke verweigern" unter "Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Wechseldatenlaufwerke".
OK
Abbrechen
Übernehmen

Abbildung 4.39 Aktivieren der Richtlinie *Wechseldatenträger: Schreibzugriff verweigern*

6. Klicken Sie auf *Standard*, um im rechten Fensterabschnitt die Registerkarte *Standard* auszuwählen. Der Editor für lokale Gruppenrichtlinien sieht nun ähnlich aus wie in Abbildung 4.34 weiter oben in dieser Lektion.
7. Klicken Sie im rechten Fensterabschnitt doppelt auf *Wechseldatenträger: Schreibzugriff verweigern*.
8. Wählen Sie *Aktiviert* aus, wie in Abbildung 4.39 gezeigt. Klicken Sie auf *OK*.
9. Überprüfen Sie, ob Sie Daten in den USB-Flashstick schreiben können. Unter Umständen müssen Sie das Gerät abziehen und erneut anstecken, damit es in der Konsole *Computer* aufgelistet wird.
10. Klicken Sie im Editor für lokale Gruppenrichtlinien doppelt auf *Wechseldatenträger: Schreibzugriff verweigern*.
11. Wählen Sie die Option *Nicht konfiguriert* aus. Klicken Sie auf *OK*.
12. Überprüfen Sie, ob es wieder möglich ist, Daten in den USB-Flashstick zu schreiben. Wie zuvor müssen Sie das Gerät möglicherweise abziehen und erneut anstecken, damit es in der Konsole *Computer* aufgelistet wird.

Übung 2 Konvertieren eines Basisdatenträgers in einen dynamischen Datenträger

Einen Basisdatenträger in einen dynamischen Datenträger zu konvertieren, ist normalerweise ein ungefährlicher Vorgang, bei dem die Daten auf dem Datenträger unversehrt bleiben. Dennoch sollten Sie eine Datensicherung aller wichtigen Dateien auf dem Datenträger durchführen, bevor Sie diese Übung in Angriff nehmen. Falls Sie zwei Datenträger in Ihrem Computer haben, sollten Sie den verwenden, der nicht das Betriebssystem enthält.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Klicken Sie im Menü *Alle Programme/Zubehör* mit der rechten Maustaste auf *Eingabeaufforderung* und wählen Sie den Befehl *Als Administrator ausführen*. Klicken Sie bei Bedarf auf *Ja*, um das UAC-Dialogfeld zu bestätigen.
3. Geben Sie **diskpart** ein.
4. Geben Sie an der DISKPART>-Eingabeaufforderung **list disk** ein und notieren Sie sich die Nummer des Datenträgers, den Sie konvertieren wollen.

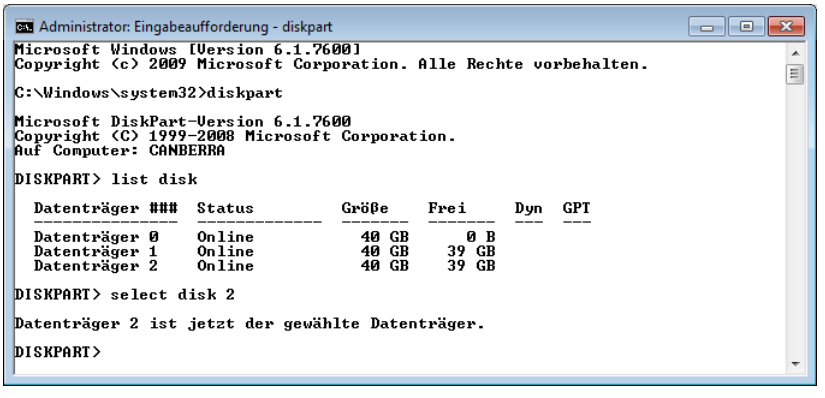

Administrator: Eingabeaufforderung - diskpart
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Windows\system32>diskpart
Microsoft DiskPart-Version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
Auf Computer: CANBERRA
DISKPART> list disk
Datenträger ### Status Größe Frei Dyn GPT
Datenträger 0 Online 40 GB 0 B
Datenträger 1 Online 40 GB 39 GB
Datenträger 2 Online 40 GB 39 GB
DISKPART> select disk 2
Datenträger 2 ist jetzt der gewählte Datenträger.
DISKPART>

Abbildung 4.40 Auswählen eines Datenträgers, der konvertiert werden soll

5. Geben Sie an der DISKPART>-Eingabeaufforderung **select disk <*Datenträgernummer*>** ein. Ihr Bildschirm müsste nun ähnlich aussehen wie in Abbildung 4.40.
6. Geben Sie an der DISKPART>-Eingabeaufforderung **convert dynamic** ein.

Zusammenfassung der Lektion

- Sie können die Konsole *Datenträgerverwaltung* oder das Befehlszeilentool Diskpart verwenden, um Datenträger, Partitionen und Volumes auf einem Windows 7-Computer zu verwalten.
- Mit Gruppenrichtlinien können Sie den Zugriff auf Wechselmediengeräte steuern.
- Windows 7 unterstützt Basisdatenträger, dynamische Datenträger sowie die Partitionsstile MBR und GPT. Sie können diese Datenträgertypen von einem in den anderen konvertieren.
- Windows 7 stellt Software-RAID-0, -RAID-1 und -RAID-5-Volumes zur Verfügung. Sie können außerdem einfache und übergreifende Volumes erstellen. Sie können ein Volume verkleinern oder vergrößern, ohne auf Tools anderer Hersteller zurückzugreifen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Verwalten von Datenträgern«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welcher Diskpart-Befehl konvertiert einen MBR- in einen GPT-Datenträger?
   A. `convert gpt`
   B. `convert mbr`
   C. `convert basic`
   D. `convert dynamic`
2. Sie brauchen Fehlertoleranz für Ihr Betriebssystem, damit Ihr Computer mit Windows 7 Home Premium auch dann noch startet, wenn eine Festplatte ausfällt. Sie haben zwei Festplatten, auf der zweiten ist ein Bereich noch nicht zugewiesen. Wie gehen Sie vor?
   A. Erstellen Sie eine VHD und installieren Sie ein Abbild Ihres Computers auf der VHD. Machen Sie die VHD mit BCDEdit startfähig.
   B. Erstellen Sie ein RAID-0-Volume.
   C. Erstellen Sie ein RAID-1-Volume.
   D. Erstellen Sie ein RAID-5-Volume.

3. Sie wollen Lese-, Schreib- und Ausführungszugriff auf alle Arten externer Speichergeräte verhindern. Welche Gruppenrichtlinie aktivieren Sie?
   A. *Alle Wechselmedien: Jeglichen direkten Zugriff in Remotesitzungen verweigern*
   B. *Alle Wechselmedienklassen: Jeglichen Zugriff verweigern*
   C. *Wechseldatenträger: Lesezugriff verweigern*
   D. *Wechseldatenträger: Schreibzugriff verweigern*
4. Sie erstellen mit dem Tool Diskpart ein RAID-0-Volume in nicht zugewiesenen Bereichen auf Datenträger 1, 2 und 3. Sie wollen das Volume so groß wie möglich machen. Welchen Befehl geben Sie ein?
   A. `create volume stripe size=0 disk=1,2,3`
   B. `create volume stripe disk=1,2,3`
   C. `create volume raid size=0 disk=1,2,3`
   D. `create volume raid disk=1,2,3`
5. Sie bauen einen dynamischen Datenträger aus dem Windows 7-Computer *Canberra* aus und in den Windows 7-Computer *Aberdeen* ein. Dem Datenträger war auf *Canberra* der Laufwerkbuchstabe *H:* zugewiesen. Auf *Aberdeen* sind bereits die Laufwerke *C:*, *D:* und *E:* vorhanden. Sie haben *Aberdeen* nicht so konfiguriert, dass keine neuen Volumes zum System hinzugefügt werden dürfen. Welchen Laufwerkbuchstaben bekommt der Datenträger auf *Aberdeen* zugewiesen?
   A. Der Datenträger wird nicht eingebunden und bekommt keinen Laufwerkbuchstaben zugewiesen.
   B. *F:*
   C. *G:*
   D. *H:*

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Ist ein Gerät nicht PnP-fähig, müssen Sie Administratoranmeldeinformationen eingeben, um es zu installieren. Sie können einen Gerätetreiber vorab bereitstellen und (sofern nötig) digital signieren, damit Nicht-Administratoren ihn installieren können.
- Sie können verhindern, dass Treiber automatisch aus Windows Update heruntergeladen und installiert werden. Sie können die Windows Update-Site auch ganz aus dem Suchpfad für Gerätetreiber entfernen, die nicht im Gerätetreiberspeicher vorhanden sind. Sie können Gerätetreiber aktualisieren, deaktivieren (oder beenden), deinstallieren oder die Vorversion wiederherstellen.
- Sie können in Windows 7 Datenträger, Partitionen und Volumes verwalten und den Zugriff auf Wechselmediengeräte steuern. Sie können einen Datenträgertyp in einen anderen Typ und einen anderen Partitionsstil konvertieren. Sie können Volumes verkleinern oder vergrößern.
- Windows 7 unterstützt einfache, übergreifende, RAID-0-, RAID-1- und RAID-5-Volumes.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Defragmentierung**
- **Treiberspeicher**
- **Staging**
- **RAID (Redundant Array of Independent Disks)**
- **Speicher *Vertrauenswürdige Herausgeber***

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie an, was Sie über das Verwalten von Geräten und Datenträgern gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Erzwingen einer Treibersignierungsrichtlinie

Sie sind leitender Systemadministrator bei der Firma A. Datum. Eine schriftlich festgehaltene Unternehmensrichtlinie fordert, dass im Produktivnetzwerk nur Treiber installiert werden dürfen, die alle WHQL-Tests bestanden haben und von Microsoft digital signiert sind. Sie betreiben ein Testnetzwerk, das vollständig vom Produktivnetzwerk getrennt ist, in dem Sie Software testen, darunter auch bisher unsignierte Gerätetreiber. Sie vermuten, dass einer Ihrer Mitarbeiter einen unsignierten Treiber auf einem Computer im Produktivnetzwerk installiert hat und deshalb die Grafikkarte auf dem betroffenen Computer nicht richtig funktioniert.

Beantworten Sie die folgenden Fragen:

1. Wie können Sie die DirectX-Grafikkarte prüfen und feststellen, ob der Treiber nicht die WHQL-Tests durchlaufen hat oder ob andere Probleme bestehen?
2. Wie prüfen Sie, ob noch andere unsignierte Treiber auf dem Computer installiert sind?
3. Angenommen, das Problem wird nicht durch den Treiber verursacht, mit welchem Tool stellen Sie dann fest, ob ein Ressourcenkonflikt mit anderer Hardware vorliegt?
4. Der unsignierte Treiber, um den es hier geht, hat in Ihrem Testnetzwerk einwandfrei funktioniert. Sie wollen ihn erneut gründlich testen, diesmal unter Stressbedingungen wie knappen Ressourcen. Welches Tool steht Ihnen dafür zur Verfügung?

Übung mit Fallbeispiel 2: Verwalten von Datenträgern

Sie haben einen Computer mit Windows 7 Enterprise eingerichtet und drei zusätzliche Festplatten eingebaut. Datenträger 0 ist die ursprüngliche Festplatte. Sie enthält das Betriebssystem auf Laufwerk *C:*. Dies ist eine 200-GByte-Festplatte, auf der es keinen nicht zugewiesenen Platz mehr gibt. Datenträger 1 ist eine 200-GByte-Festplatte, Datenträger 2 eine 400-GByte-Festplatte und Datenträger 3 eine 200-GByte-Festplatte. Momentan ist der gesamte Platz auf den Datenträgern 1, 2 und 3 nicht zugewiesen. Sie wollen Fehlertoleranz sowohl für Ihr Betriebssystem als auch die Daten erreichen. Außerdem wollen Sie den Zugriff auf die Daten beschleunigen.

Beantworten Sie die folgenden Fragen:

1. Welche Art Volume erstellen Sie für Ihr Betriebssystem, und auf welchen Datenträgern legen Sie das Volume an?
2. Welche Art Volume erstellen Sie zum Speichern Ihrer Daten, und auf welchen Datenträgern legen Sie dieses Volume an?
3. Prüfen Sie, ob Ihre Antwort auf Frage 2 stimmt. Welche Kapazität steht für die Datenspeicherung auf Ihrem Datenvolume zur Verfügung?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Untersuchen der Gruppenrichtlinien, die für die Verwaltung der Geräteinstallation zur Verfügung stehen

- **Übung 1** Machen Sie sich mit den verfügbaren Richtlinien im Editor für lokale Gruppenrichtlinien vertraut. Klicken Sie doppelt auf jede Richtlinie, um die detaillierte Beschreibung zu lesen. Erweitern Sie die Zweige *Computerverwaltung*, *Administrative Vorlagen* sowie *System* und sehen Sie sich vor allem die Richtlinien unter *Wechselmedienzugriff*, *Treiberinstallation*, *Geräteinstallation* und *Einschränkungen bei der Geräteinstallation* an.

Arbeiten mit dem Treiberüberprüfungs-Manager

- **Übung 1** Testen Sie mit dem Treiberüberprüfungs-Manager einen ausgewählten Treiber unter Stressbedingungen. Wenn Sie vorhaben, ein Gerät von einem anderen Hersteller zu installieren, das nicht PnP-fähig ist, können Sie im Treiberüberprüfungs-Manager den vom Hersteller zur Verfügung gestellten Treiber testen.

Verwenden von Diskpart

- **Übung 1** Das Tool Diskpart erledigt viele Aufgaben im Bereich der Datenträgerverwaltung. Arbeiten Sie mit dem Tool, bis sie mit seinen Parametern und Abläufen vertraut sind. Üben Sie beispielsweise, wie Sie einen Datenträger oder ein Volume auswählen, bevor Sie Operationen damit ausführen. Sehen Sie sich an, wie Sie Skripts schreiben, die das Tool aufrufen, und welche Rolle das Argument `noerr` dabei spielt.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

KAPITEL 5

Verwalten von Anwendungen

Einer der wichtigsten Aspekte beim Wechsel auf ein neues Betriebssystem ist, dafür zu sorgen, dass alle Anwendungen, die auf dem alten Betriebssystem funktioniert haben und für die tägliche Arbeit gebraucht werden, auch auf dem neuen Betriebssystem funktionieren. Der Wechsel auf ein neues Betriebssystem wird gewöhnlich aus gutem Grund nicht durchgeführt, wenn er den Ausfall der Anwendungen bedeutet, die für die tägliche Arbeit unerlässlich sind. Kompatibilität ist ein entscheidender Punkt für die Akzeptanz von Windows 7, weil viele Organisationen noch Windows XP verwenden. Manche Anwendungen, die für Windows XP entwickelt wurden, laufen wegen Kompatibilitätsproblemen nicht auf Windows 7. Windows 7 enthält einige Anwendungskompatibilitätsfunktionen, mit denen Administratoren das Betriebssystem so konfigurieren können, dass sich diese älteren Anwendungen auch nach einem Wechsel auf Windows 7 noch verwenden lassen.

Ebenso wichtig wie die Verwendbarkeit der unverzichtbaren Anwendungen auf einem neuen Betriebssystem ist es, Benutzer an der Ausführung nicht genehmigter Anwendungen zu hindern, die sich störend auf die Arbeit auswirken können. Es gibt viele Gründe dafür, nur die Verwendung von ausdrücklich genehmigten Anwendungen auf einem Computer zuzulassen, angefangen beim Schutz der Benutzer vor ablenkenden Spielchen bis hin zum Schutz der Umgebung vor Malware. Wenn nur genehmigte Anwendungen ausgeführt werden können, lassen sich nicht genehmigte Anwendungen wie Malware, Spiele und Filesharingprogramme automatisch nicht mehr ausführen.

In diesem Kapitel erfahren Sie, wie Sie Anwendungskompatibilitätsprobleme beheben können, angefangen bei der Verwendung der vordefinierten Kompatibilitätsmodi von Windows 7 bis hin zur Verwendung der Virtualisierungsoption Windows XP Mode. Außerdem erfahren Sie, wie Sie mit AppLocker und den Richtlinien für Softwareeinschränkung festlegen, welche Anwendungen in Ihrer Organisation unter Windows 7 verwendet werden können.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren der Anwendungskompatibilität
- Konfigurieren von Anwendungseinschränkungen

Lektionen in diesem Kapitel:

- Lektion 1: Anwendungskompatibilität 255
- Lektion 2: Verwalten von AppLocker und der Richtlinien für Softwareeinschränkung 269

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels sind einige Vorbereitungen erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Client-PC namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.
- Laden Sie den Process Explorer von der Microsoft-Website herunter. Sie finden ihn unter *http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx.*

Praxistipp

Orin Thomas

Die Richtlinien für Softwareeinschränkung gehören zu den Dingen, die sich in der Theorie als großartige Idee darstellen, aber in der Praxis nur mit großem Zeitaufwand umsetzbar sind. Die Theorie besagt, dass Sie mit den Richtlinien für Softwareeinschränkung eine Liste der Anwendungen festlegen können, die sich auf den Computern Ihrer Organisation ausführen lassen. Steht die Anwendung nicht in der Liste, kann sie nicht ausgeführt werden. In der Praxis bedeutet dies, dass Sie herausfinden müssen, welche ausführbaren Dateien Sie auf den Computern zulassen wollen. Das ist keine einfache Sache, denn es gibt im Windows-Ordner eine ganze Reihe von Anwendungen, die für die Funktionsfähigkeit des Computers unerlässlich sind. Die strengste Softwarebeschränkungsregel ist die Hashregel. Sie verwendet zur Identifizierung einer Datei so etwas wie einen digitalen »Fingerabdruck«. Um Hashregeln verwenden zu können, müssen Sie für jede ausführbare Datei aus Ihrer Zulassungsliste manuell einen digitalen Fingerabdruck erstellen. Das dauert noch länger als die Aufstellung der Liste. Nach jeder Aktualisierung der Software mit einem Patch müssen Sie die Hashwerte aller ausführbaren Dateien neu berechnen, die bei dieser Aktualisierung geändert wurden, weil die alten digitalen Fingerabdrücke nicht mehr zu den geänderten Dateien passen. Die Aufstellung der Zulassungsliste und die Berechnung und Neuberechnung der Hashwerte gehören zu den Dingen, die auch ein sehr auf Sicherheit bedachter Administrator als etwas umständlich oder langweilig einstufen wird. Das Ergebnis ist zwar eine sehr sichere Umgebung, aber es erfordert viel Arbeit, diese Sicherheit aufrechtzuerhalten. AppLocker, eingeführt mit Windows 7 und Windows Server 2008 R2, verringert deutlich den Arbeitsaufwand für die Aufstellung der Zulassungsliste. Es gibt Assistenten, mit denen sich die Erstellung der Hashregeln automatisieren lässt. Außerdem gibt es verbesserte Herausgeberregeln, mit denen Sie eine bestimmte Anwendung und alle nachfolgenden Versionen der Anwendung zulassen können. Sie können einen Referenzcomputer aufbauen und dann für jede ausführbare Datei, die sich auf diesem Computer befindet, automatisch Regeln erstellen. Auf diese Weise wird aus einer Idee, die in der Theorie gut klingt, eine Idee, die auch in der Praxis etwas taugt.

Lektion 1: Anwendungskompatibilität

Zwischen Windows 7 und älteren Windows-Clientbetriebssystemen gibt es große Unterschiede. Verbesserungen im Bereich der Anwendungssicherheit mit Funktionen wie der Datenausführungsverhinderung und der obligatorischen Integritätskontrolle (Mandatory Integrity Control) haben allerdings auch die Wirkung, dass Anwendungen, die in älteren Windows-Versionen bestimmte Dinge tun, dies unter Windows 7 nicht mehr tun können. Daraus können sich, wie bereits erwähnt, für Administratoren beim Wechsel auf Windows 7 Probleme ergeben. In dieser Lektion erfahren Sie, wie Sie Anwendungskompatibilitätsprobleme beheben können, damit sich Anwendungen, die auf älteren Windows-Versionen funktionierten, auch unter Windows 7 verwenden lassen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren der Kompatibilitätsmodi für Anwendungen
- Beheben von Kompatibilitätsproblemen mit dem Application Compatibility Toolkit (ACT)
- Erkennen von Kompatibilitätsproblemen des Internet Explorers mit dem Internet Explorer Compatibility Test Tool.

Veranschlagte Zeit für diese Lektion: 40 Minuten

Konfigurieren der Kompatibilitätsoptionen

Viele Anwendungen, die unter Windows XP funktionieren, laufen zwar auch unter Windows 7 problemlos, eine kleine Anzahl wichtiger Anwendungen allerdings nicht. Es gibt verschiedene Wege, solche Anwendungen unter Windows 7 zum Laufen zu bringen, angefangen bei der automatischen Einstellung der Konfigurationsoptionen mit der Problembehandlung für Programmkompatibilität bis hin zum Betrieb der Anwendung in Windows XP Mode, einer virtualisierten Betriebssystemumgebung. Wichtig ist, dass es Möglichkeiten gibt, auch eine inkompatible Anwendung unter Windows 7 zum Laufen zu bringen. Allerdings kann dafür ein gewisser Zeit- und Arbeitsaufwand erforderlich werden.

Die Problembehandlung für Programmkompatibilität

Die Problembehandlung für Programmkompatibilität (Abbildung 5.1) führt eine Reihe von Tests mit einer Anwendung durch und versucht dann, die richtigen Kompatibilitätseinstellungen automatisch vorzunehmen. Das ist die einfachste Methode zur Behebung von Kompatibilitätsproblemen, weil die Probleme vom Betriebssystem automatisch behoben werden. Wenn die Problembehandlung für Programmkompatibilität eine Lösung gefunden hat, wird diese Lösung gespeichert und die Anwendung wird sich auch zukünftig verwenden lassen, ohne wieder dieselben Probleme zu verursachen.

Die Problembehandlung für Programmkompatibilität funktioniert nur bei ausführbaren Dateien. Um sie zu starten, klicken Sie die betreffende Programmdatei oder eine entsprechende Verknüpfung mit der rechten Maustaste an und wählen *Behandeln von Kompatibilitätsproblemen*. Mit der Problembehandlung für Programmkompatibilität können Sie keine Probleme beheben, die sich bei der Installation mit einer Installationsdatei ergeben, die im MSI-Format vorliegt. Die Problembehandlung für Programmkompatibilität löst die meisten häufiger auftretenden Kompatibilitätsprobleme. Kann die Problembehandlung für Programm-

kompatibilität ein Kompatibilitätsproblem nicht beheben, versuchen Sie es mit der nächsten Methode, nämlich mit der manuellen Konfiguration eines vordefinierten Kompatibilitätsmodus.

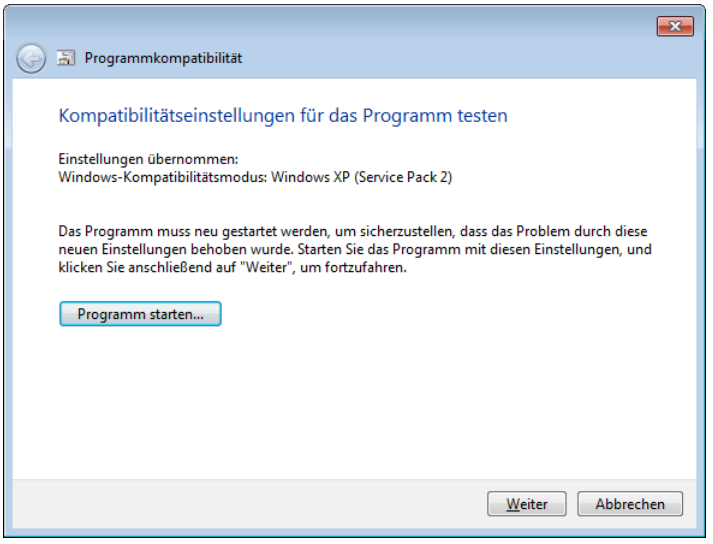

Programmkompatibilität
Kompatibilitätseinstellungen für das Programm testen
Einstellungen übernommen:
Windows-Kompatibilitätsmodus: Windows XP (Service Pack 2)
Das Programm muss neu gestartet werden, um sicherzustellen, dass das Problem durch diese neuen Einstellungen behoben wurde. Starten Sie das Programm mit diesen Einstellungen, und klicken Sie anschließend auf "Weiter", um fortzufahren.
Programm starten...
Weiter
Abbrechen

Abbildung 5.1 Die Problembehandlung für Programmkompatibilität

Vordefinierte Kompatibilitätsmodi und Optionen

Windows 7 bietet einige vordefinierte Kompatibilitätsmodi, mit denen sich bestimmte Aspekte eines älteren Betriebssystems nachahmen lassen, damit die fragliche Anwendung lauffähig wird. Allerdings funktioniert nicht jede Anwendung unter Windows 7, die auf einem älteren Betriebssystem lauffähig war, auch wenn Sie die entsprechenden Kompatibilitätseinstellungen vornehmen. Um die Einstellungen vorzunehmen, öffnen Sie das Eigenschaftendialogfeld der Anwendung und wechseln auf die Registerkarte *Kompatibilität* (Abbildung 5.2).

In der Dropdownliste können Sie einen der folgenden Kompatibilitätsmodi auswählen:

- *Windows 95*
- *Windows 98 / Windows Me*
- *Windows NT 4 (Service Pack 5)*
- *Windows 2000*
- *Windows XP (Service Pack 2)*
- *Windows XP (Service Pack 3)*
- *Windows Server 2003 (Service Pack 1)*
- *Windows Server 2008 (Service Pack 1)*
- *Windows Vista*
- *Windows Vista (Service Pack 1)*
- *Windows Vista (Service Pack 2)*

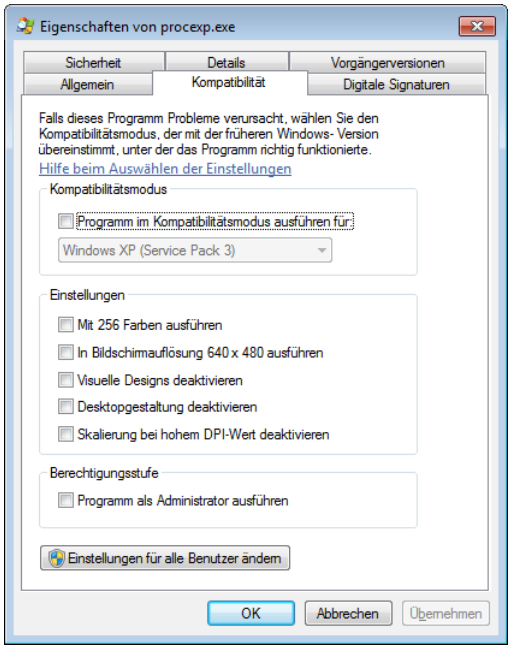


Abbildung 5.2 Verfügbare Kompatibilitätsmodi

Außerdem sind auf derselben Registerkarte noch einige Kompatibilitätsoptionen verfügbar:

- **Mit 256 Farben ausführen** Ermöglicht die Verwendung von Anwendungen, die für eine eingeschränkte Farbpalette ausgelegt sind.
- **In Bildschirmauflösung 640 x 480 ausführen** Ermöglicht die Verwendung von Anwendungen, die für eine niedrige Auflösung ausgelegt sind und keine höhere Auflösung bieten.
- **Visuelle Designs deaktivieren** Visuelle Designs können in manchen Anwendungen zu Problemen mit der Darstellung von Menüs und Schaltflächen führen. Die Aktivierung dieser Einstellung kann diese Probleme beheben.
- **Desktopgestaltung deaktivieren** Deaktiviert Leistungsmerkmale der Benutzeroberfläche Aero, beispielsweise die Transparenz, solange die Anwendung aktiv ist.
- **Skalierung bei hohem DPI-Wert deaktivieren** Deaktiviert die automatische Größenanpassung von Anwendungsfenstern, wenn große Schriftarten verwendet werden. Diese Einstellung sollte aktiviert werden, wenn sich große Schriftarten negativ auf das Erscheinungsbild der Anwendung auswirken.
- **Programm als Administrator ausführen** Einige ältere Programme, die erhöhte Rechte brauchen, sind nicht in der Lage, diese Rechte anzufordern. Bei diesem Vorgang öffnet sich gewöhnlich ein Dialogfeld der Benutzerkontensteuerung. Durch die Aktivierung dieser Option wird das Programm als Administrator ausgeführt. Das bedeutet, dass nur Benutzer, die auf dem Computer über Administratorrechte verfügen, das Programm verwenden können.
- **Einstellungen für alle Benutzer ändern** Standardmäßig gelten Kompatibilitätsoptionen nur für den angemeldeten Benutzer. Nach einem Klick auf die Schaltfläche

Einstellungen für alle Benutzer ändern können Sie Kompatibilitätseinstellungen für alle Benutzer des Computers vornehmen.

Die Problembehandlung für Programmkompatibilität probiert diese Einstellungen durch, um die Anwendung zum Laufen zu bringen. Hat sie damit keinen Erfolg, kommen Sie vielleicht weiter, wenn Sie die Einstellungen von Hand vornehmen. Für Anwendungen aus dem Betriebssystem Windows können Sie keine Kompatibilitätseinstellungen vornehmen. Falls Sie auch mit diesen Einstellungen keinen Erfolg haben, können Sie mit dem ACT einen benutzerdefinierten Kompatibilitätsmodus festlegen, der sich für die fragliche Anwendung besser eignet.

Schnelltest

- Welche Kompatibilitätsoption sollten Sie für ein Programm aktivieren, das erhöhte Rechte braucht, aber eine Bestätigungsaufforderung der Benutzerkontensteuerung auslöst?

Antwort zum Schnelltest

- Sie sollten die Option *Programm als Administrator ausführen* aktivieren, weil die Anwendung dann mit erhöhten Rechten ausgeführt werden kann. Der Benutzer sieht die Bestätigungsaufforderung der Benutzerkontensteuerung, bevor die Anwendung die erhöhten Rechte erhält.

Das Application Compatibility Toolkit

Das Application Compatibility Toolkit (ACT) ist eine Sammlung von Tools zur Behebung von Anwendungskompatibilitätsproblemen. Mit dem ACT können Sie überprüfen, ob vorhandene Anwendungen zu Windows 7 kompatibel sind, bevor Sie das neue Betriebssystem bereitstellen.

Das ACT enthält folgende Komponenten:

- Application Compatibility Manager
- Compatibility Administrator
- Internet Explorer Compatibility Test Tool
- Setup Analysis Tool
- Standard User Analyzer

Im weiteren Verlauf dieser Lektion erfahren Sie mehr über diese Tools.



Weitere Informationen ACT

Sie erhalten das ACT im Microsoft Download Center unter *http://download.microsoft.com*. Suchen Sie nach dem Toolkit mit seinem Namen.

Application Compatibility Manager

Der Application Compatibility Manager (Abbildung 5.3) ermöglicht die Sammlung und Analyse von Kompatibilitätsdaten, damit Sie Probleme vor der Bereitstellung von Windows 7 in Ihrer Organisation erkennen und beheben können. Die erfassten Daten werden in einer Microsoft SQL Server-Datenbank gespeichert. Mit dem Application Compatibility Manager

können Sie Datensammlungspakete (Data Collection Package, DCP) erstellen und bereitstellen. Datensammlungspakete sammeln auf den vorgesehenen Clientcomputern Daten über Hardware, Software und Geräte. Diese Daten werden über den Application Compatibility Manager an eine SQL Server-Datenbank weitergeleitet, die im Netzwerk verfügbar sein muss, wenn Sie dieses Tool verwenden möchten. Durch eine Analyse der Daten aus der Datenbank können Sie erkennen, welche Kompatibilitätsprobleme sich wahrscheinlich bei den in der Organisation verwendeten Anwendungen ergeben werden.

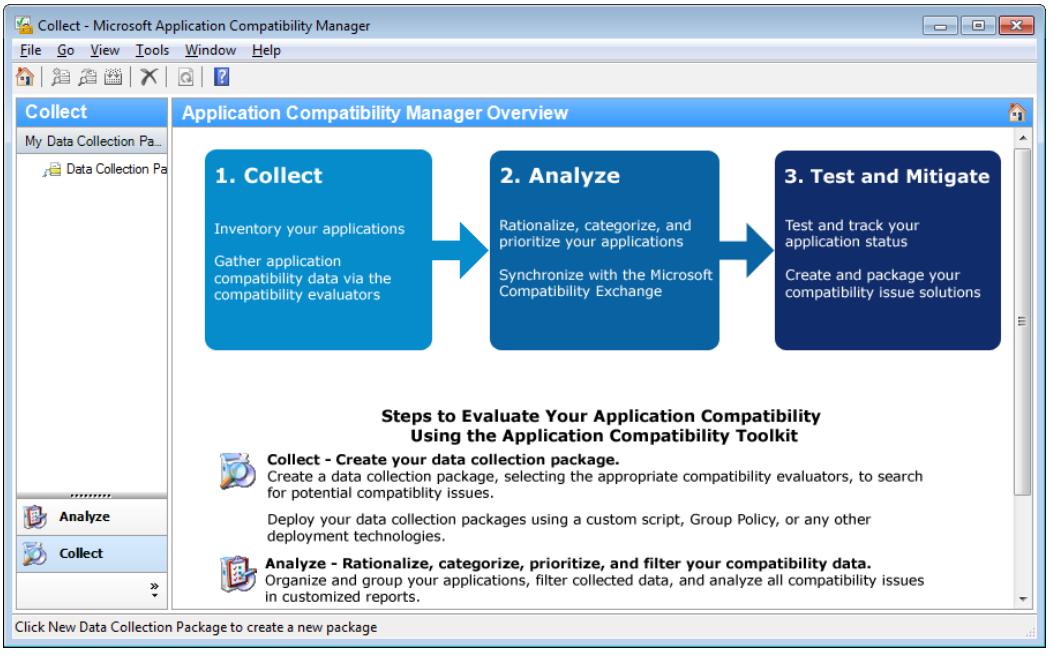

Collect - Microsoft Application Compatibility Manager
File Go View Tools Window Help
Collect
My Data Collection Pa...
Data Collection Pa
Analyze
Collect
Application Compatibility Manager Overview
1. Collect
Inventory your applications
Gather application compatibility data via the compatibility evaluators
2. Analyze
Rationalize, categorize, and prioritize your applications
Synchronize with the Microsoft Compatibility Exchange
3. Test and Mitigate
Test and track your application status
Create and package your compatibility issue solutions
Steps to Evaluate Your Application Compatibility Using the Application Compatibility Toolkit
Collect - Create your data collection package.
Create a data collection package, selecting the appropriate compatibility evaluators, to search for potential compatiblity issues.
Deploy your data collection packages using a custom script, Group Policy, or any other deployment technologies.
Analyze - Rationalize, categorize, prioritize, and filter your compatibility data.
Organize and group your applications, filter collected data, and analyze all compatibility issues in customized reports.
Click New Data Collection Package to create a new package

Abbildung 5.3 Der Application Compatibility Manager

Compatibility Administrator

Der Compatibility Administrator (Abbildung 5.4) ermöglicht die Behebung einer großen Zahl von Anwendungskompatibilitätsproblemen, die sich bei der Bereitstellung vorhandener älterer Anwendungen auf Windows 7 ergeben könnten. Der Compatibility Administrator bietet eine Sammlung von einzelnen Kompatibilitätsfixes und Kompatibilitätsmodi, die sich zur Behebung von Problemen der vorhandenen Software verwenden lassen. Für eine große Zahl von Anwendungen gibt es bereits Kompatibilitätsfixes, die den Einsatz dieser Anwendung unter Windows 7 ermöglichen. Überprüfen Sie zuerst hier, ob es für die Anwendung, die Sie interessiert, bereits eine Lösung gibt.

Ist in der Datenbank keine Lösung vorhanden, können Sie Ihre eigenen Kompatibilitätsfixes, -modi und -datenbanken erstellen, um Anwendungskompatibilitätsprobleme zu beheben. Ein *Kompatibilitätsfix* (in der englischen Fachliteratur auch *shim* genannt) ist eine dünne Softwareschicht, die API-Aufrufe (Application Programming Interface) von Anwendungen abfängt und so ändert, dass die Anwendung eine ähnliche Antwort erhält wie unter einer älteren Windows-Version. Ein *Kompatibilitätsmodus* ist eine Sammlung von Kompatibilitätsfixes.

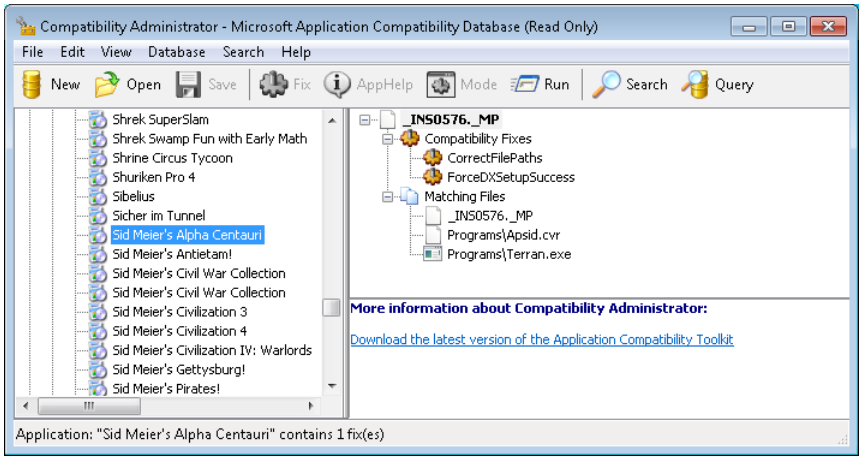


Abbildung 5.4 Der Compatibility Administrator zeigt einen vorhandenen Fix an

Internet Explorer Compatibility Test Tool

Mit dem Internet Explorer Compatibility Test Tool (Abbildung 5.5) können Sie überprüfen, ob es Kompatibilitätsprobleme mit Websites gibt, die sich darauf auswirken, wie diese Websites im Internet Explorer 8 dargestellt werden. Das ist die Version, die mit Windows 7 ausgeliefert wird. Da viele Organisationen in ihrem Intranet Webanwendungen verwenden, ohne die sie nicht arbeiten können, ist es wichtig, Kompatibilitätsprobleme nicht nur mit herkömmlichen Anwendungen zu beheben, sondern auch mit Webanwendungen.

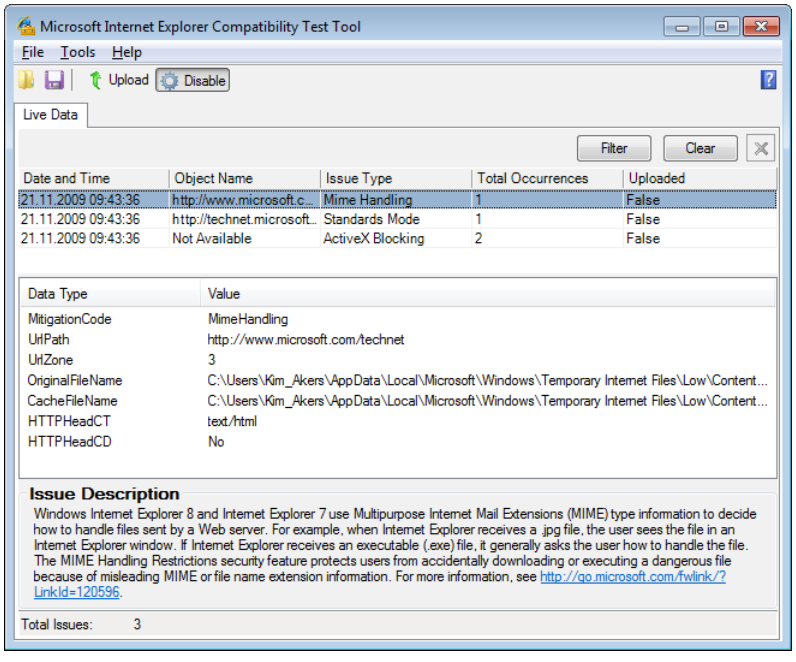

Microsoft Internet Explorer Compatibility Test Tool
File Tools Help
Upload Disable
Live Data
Filter Clear
Date and Time Object Name Issue Type Total Occurrences Uploaded
21.11.2009 09:43:36 http://www.microsoft.c... Mime Handling 1 False
21.11.2009 09:43:36 http://technet.microsoft... Standards Mode 1 False
21.11.2009 09:43:36 Not Available ActiveX Blocking 2 False
Data Type Value
MitigationCode MimeHandling
UrlPath http://www.microsoft.com/technet
UrlZone 3
OriginalFileName C:\Users\Kim_Akers\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content...
CacheFileName C:\Users\Kim_Akers\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content...
HTTPHeadCT text/html
HTTPHeadCD No
Issue Description
Windows Internet Explorer 8 and Internet Explorer 7 use Multipurpose Internet Mail Extensions (MIME) type information to decide how to handle files sent by a Web server. For example, when Internet Explorer receives a .jpg file, the user sees the file in an Internet Explorer window. If Internet Explorer receives an executable (.exe) file, it generally asks the user how to handle the file. The MIME Handling Restrictions security feature protects users from accidentally downloading or executing a dangerous file because of misleading MIME or file name extension information. For more information, see http://go.microsoft.com/fwlink/?LinkId=120596.
Total Issues: 3

Abbildung 5.5 Das Internet Explorer Compatibility Test Tool

Um das Internet Explorer Compatibility Test Tool zu verwenden, öffnen Sie es im Untermenü *Developer and Tester Tools* des Menüs *Microsoft Application Compatibility Toolkit* aus dem *Start*-Menü, klicken auf *Enable* und öffnen den Internet Explorer. Dann erscheint ein Hinweis, der Sie darüber informiert, dass die Kompatibilitätsevaluierung eingeschaltet ist. Besuchen Sie die Websites und verwenden Sie die Webanwendungen, die Sie überprüfen möchten. Das Tool zeichnet mögliche Kompatibilitätsprobleme auf.

Setup Analysis Tool

Das Setup Analysis Tool überwacht die Aktivitäten von Installationsprogrammen und kann folgende Kompatibilitätsprobleme erkennen:

- Installation von Kernelmodustreibern
- Installation von 16-Bit-Komponenten
- Installation von GINA-DLLs (Graphical Identification and Authentication Dynamic-Link Libraries)
- Änderung von Dateien oder Registrierungsschlüsseln, die vom Windows-Ressourcenschutz geschützt werden

Zur Durchführung einer Untersuchung öffnen Sie das Setup Analysis Tool und geben den Speicherort der Installationsdatei ein, die Sie überprüfen möchten. Das Setup Analysis Tool führt das Installationsprogramm aus und überprüft, welche Probleme während der Installation auftreten könnten.

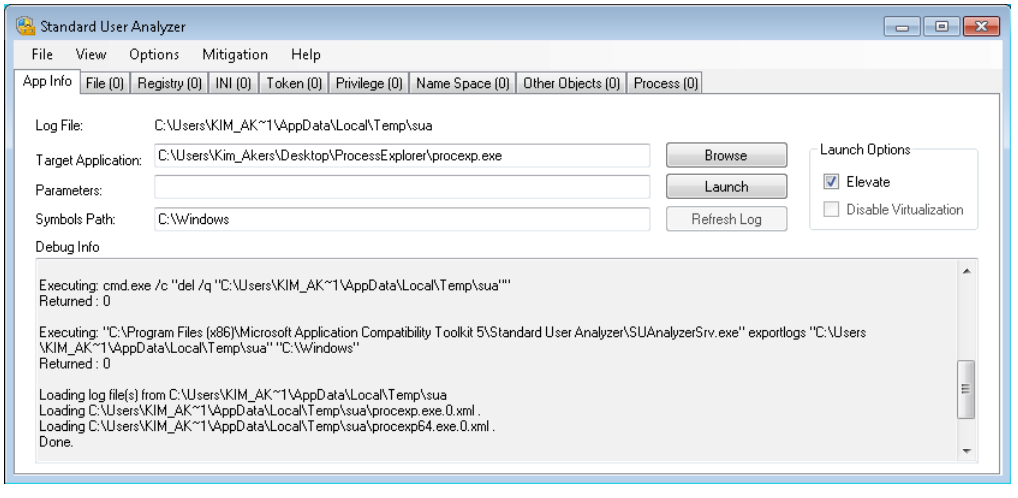


Abbildung 5.6 Standard User Analyzer

Standard User Analyzer

Der Standard User Analyzer (Abbildung 5.6) ermöglicht die Überprüfung, ob sich für eine Anwendung Kompatibilitätsprobleme durch die Benutzerkontensteuerung ergeben. Er liefert Daten über problematische Dateien sowie APIs, Registrierungsschlüssel, *.ini*-Dateien, Token, Berechtigungen, Namespaces, Prozesse und andere Elemente, die von der Anwendung benutzt werden und unter Windows 7 zu Problemen führen können. Um den Standard User Analyzer zu verwenden, starten Sie ihn, geben die Zielanwendung ein und klicken dann auf

Launch. Die Anwendung versucht zu starten und der Standard User Analyzer überprüft, wie sich die Anwendung in der Windows 7-Umgebung verhält.



Weitere Informationen ACT

Weitere Informationen über das ACT erhalten Sie im folgenden Artikel der Zeitschrift TechNet Magazine: *http://technet.microsoft.com/en-us/magazine/dd797545.aspx*.

Richtlinien zur Anwendungskompatibilitätsdiagnose

Es gibt zum Thema Anwendungskompatibilität sechs Gruppenrichtlinien, die sich beim Auftreten eines Anwendungskompatibilitätsproblems auf die Reaktion von Windows 7 auswirken. Diese Richtlinien sind in einem Gruppenrichtlinienobjekt im Knoten *Computerkonfiguration\Administrative Vorlagen\System\Problembehandlung und Diagnose\Anwendungskompatibilitätsdiagnose* zu finden (Abbildung 5.7).

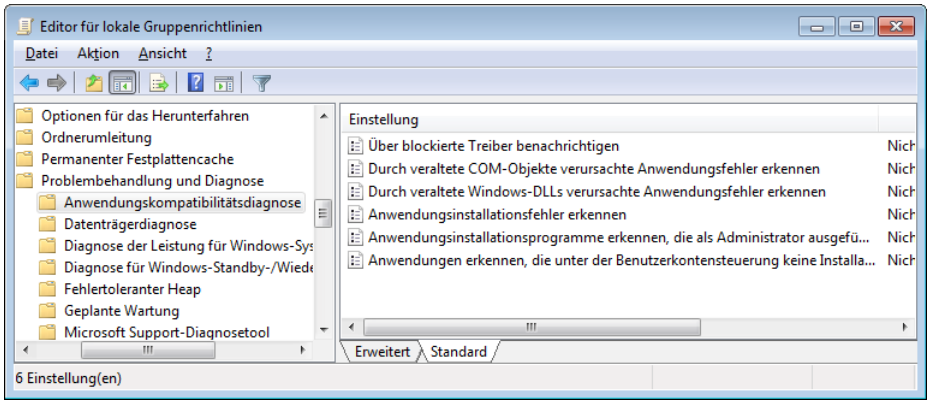


Abbildung 5.7 Richtlinien zur Anwendungskompatibilitätsdiagnose

Diese Richtlinien haben folgende Aufgaben:

- **Über blockierte Treiber benachrichtigen** Wird diese Richtlinie aktiviert, informiert Windows den Benutzer, wenn ein Treiber wegen Kompatibilitätsproblemen gesperrt ist.
- **Durch veraltete COM-Objekte verursachte Anwendungsfehler erkennen** Wird diese Richtlinie aktiviert, informiert Windows den Benutzer, wenn ein Programm versucht, ein COM-Objekt zu erstellen, das nicht von Windows 7 unterstützt wird.
- **Durch veraltete Windows-DLLs verursachte Anwendungsfehler erkennen** Wird diese Richtlinie aktiviert, informiert Windows den Benutzer, wenn ein Programm versucht, eine Windows-DLL zu laden, die nicht von Windows 7 unterstützt wird.
- **Anwendungsinstallationsfehler erkennen** Wird diese Richtlinie aktiviert, werden Fehler bei der Anwendungsinstallation erkannt und der Benutzer hat die Wahl, die Installation im Kompatibilitätsmodus zu wiederholen.
- **Anwendungsinstallationsprogramme erkennen, die als Administrator ausgeführt werden müssen** Wird diese Richtlinie aktiviert, können Anwendungen, die deswegen nicht laufen, weil sie als Administrator ausgeführt werden müssen, mit der Option *Als Administrator ausführen* erneut gestartet werden.

- **Anwendungen erkennen, die unter der Benutzerkontensteuerung keine Installationsprogramme starten können** Diese Einstellung ähnelt der vorigen, nur wird die Anwendung nicht automatisch als Administrator ausgeführt, sondern die Benutzerkontensteuerung meldet sich, damit der Benutzer die Rechte für die Installation der Anwendung anheben kann.

Wenn Sie diese Richtlinien nicht konfigurieren, informiert Windows 7 den Benutzer über auftretende Fehler und startet in bestimmten Fällen die Problembehandlung für Programmkompatibilität. In Umgebungen, in denen Benutzer Anwendungskompatibilitätsprobleme nicht selbst lösen können, deaktivieren Administratoren häufig diese Hinweise, weil es nicht sinnvoll ist, den Benutzer über den Grund eines Anwendungsversagens zu informieren, wenn er das Problem nicht beheben kann.

Windows XP Mode für Windows 7

Windows XP Mode ist eine Kompatibilitätsoption für Windows 7 Professional, Enterprise und Ultimate, die per Download verfügbar ist. Windows XP Mode verwendet die neuste Version von Microsoft Virtual PC, um unter Windows 7 eine Installation von Windows XP auf einem virtuellen Computer auszuführen. Der Unterschied zwischen Windows XP Mode und anderen Betriebssystemvirtualisierungslösungen besteht darin, dass alle Anwendungen, die Sie auf dem Windows XP Mode-Client installieren, automatisch auch auf dem Windows 7-Hostcomputer verfügbar werden. Installieren Sie zum Beispiel auf dem Windows XP Mode-Client Microsoft Office 2000, werden in das *Start*-Menü von Windows 7 Verknüpfungen mit den Office 2000-Anwendungen eingetragen. Wenn Sie eine Anwendung starten, öffnet sie sich wie jede andere Anwendung in ihrem eigenen Fenster. Aus der Sicht des Benutzers sieht es so aus, als würde die Anwendung direkt unter Windows 7 ausgeführt.

Windows XP Mode setzt einen Prozessor voraus, der die Virtualisierung auf Hardwareebene mit einem Mechanismus wie AMD-V oder Intel VT unterstützt. Standardmäßig ist diese Option meistens deaktiviert, sie muss daher meist erst im BIOS des Computers aktiviert werden. Anschließend ist es erforderlich, den Computer vollständig auszuschalten. Die Aktivierung wird nicht wirksam, wenn Sie nach der Einstellung im BIOS nur einen Warmstart durchführen. Da der Windows XP Mode-Client 256 MByte Arbeitsspeicher beansprucht, sollte der Windows 7-Computer, auf dem Sie Windows XP Mode bereitstellen, über mindestens 2 GByte Arbeitsspeicher verfügen, also deutlich mehr als die Mindestanforderung von 1 GByte.

Zur Installation von Anwendungen, die nicht zu Windows 7 kompatibel sind, müssen Sie im Ordner *Windows Virtual PC* des *Start*-Menüs den Windows XP Mode-Client starten. Nach der Installation können Sie eine Anwendung im Ordner *Windows XP Mode-Anwendungen* des Startmenüs starten. Elemente aus diesem Ordner können Sie auch auf den Desktop oder auf die Taskleiste kopieren, um sie wie ein Windows 7-Programm direkt zu starten. Wenn Sie eine auf dem virtuellen XP installierte Anwendung direkt im *Start*-Menü von Windows 7 starten, wird das virtuelle Windows XP heruntergefahren (Abbildung 5.8).

Der Windows XP Mode bietet eine x86-Version von Windows XP Professional SP3. Windows Virtual PC unterstützt keine virtuellen x64-Clients. Das bedeutet, dass Sie Windows XP Mode oder Virtual PC nicht als Kompatibilitätslösung für x64-Anwendungen einsetzen können. Da Anwendungen nicht direkt unter Windows 7 ausgeführt werden, laufen sie unter Windows XP Mode etwas langsamer.

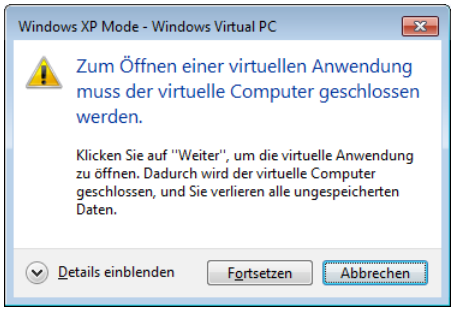

Windows XP Mode - Windows Virtual PC
Zum Öffnen einer virtuellen Anwendung muss der virtuelle Computer geschlossen werden.
Klicken Sie auf "Weiter", um die virtuelle Anwendung zu öffnen. Dadurch wird der virtuelle Computer geschlossen, und Sie verlieren alle ungespeicherten Daten.
Details einblenden
Fortsetzen
Abbrechen

Abbildung 5.8 Das virtuelle XP wird heruntergefahren, wenn eine Anwendung direkt von Windows 7 aus gestartet wird

Sie sollten den Windows XP Mode aber nur als letzte Möglichkeit betrachten, wenn es keine andere Lösung für die Kompatibilitätsprobleme der betreffenden Anwendung gibt, weil der Ressourcenbedarf wesentlich größer ist als für die vordefinierten oder benutzerdefinierten Kompatibilitätsmodi. Ein weiterer Nachteil von Windows XP Mode ist, dass Administratoren die virtuellen Windows XP-Clients wie jeden anderen Desktop-Clientcomputer ihrer Organisation pflegen und warten müssen. Das bedeutet, dass Sie die virtuellen Windows XP-Clients mit Updates auf dem neusten Stand halten müssen, auch wenn die Benutzer das Betriebssystem Windows XP gar nicht direkt verwenden.



Prüfungstipp

Eine Anwendung, die unter Windows XP SP3 einwandfrei läuft, unter Windows 7 aber nicht, wird vielleicht wieder ordnungsgemäß arbeiten, wenn Sie für diese Anwendung den Kompatibilitätsmodus Windows XP (Service Pack 3) konfigurieren.

Übung Windows 7-Kompatibilität

In dieser Übung untersuchen Sie die Windows 7-Kompatibilitätsoptionen für eine Anwendung, die Sie aus dem Internet heruntergeladen haben.

Übung Konfigurieren der Kompatibilitätsoptionen für den Process Explorer

In dieser Übung untersuchen Sie die Kompatibilitätsoptionen für eine Anwendung und überprüfen, ob die Anwendung digital signiert ist. Der Process Explorer funktioniert unter Windows 7 zwar ohne Probleme, aber Sie brauchen eine Anwendung, die nicht zum Lieferumfang von Windows 7 gehört, um Kompatibilitätsoptionen einstellen zu können. Es ist nicht möglich, Kompatibilitätsoptionen für eine Anwendung aus Windows 7 einzustellen, beispielsweise für *Calc.exe* oder *Solitaire.exe*.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an, sofern Sie nicht bereits angemeldet sind. Wenn Sie die Datei *ProcessExplorer.zip* noch nicht von der Microsoft-Website auf den Desktop heruntergeladen haben, tun Sie es jetzt.
2. Klicken Sie *ProcessExplorer.zip* mit der rechten Maustaste an und wählen Sie *Alle extrahieren*. Dadurch öffnet sich das Dialogfeld *ZIP-komprimierte Ordner extrahieren*. Übernehmen Sie den vorgeschlagenen Standardordner und die Einstellung und klicken Sie auf *Extrahieren*.

3. Klicken Sie die Anwendung *Procexp.exe* mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Klicken Sie auf *Digitale Signaturen*, wählen Sie *Microsoft Corporation* und klicken Sie dann auf *Details*. Überprüfen Sie, ob die Anwendung von Microsoft digital signiert wurde (Abbildung 5.9). Schließen Sie das Dialogfeld *Details der digitalen Signatur* mit einem Klick auf *OK*.

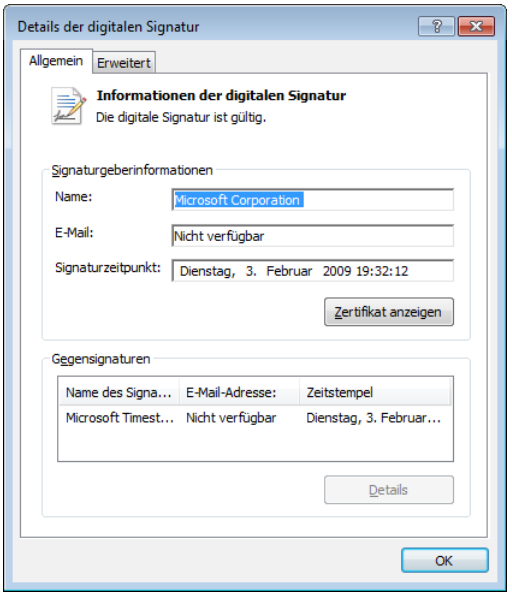


Abbildung 5.9 Überprüfen der digitalen Signatur

4. Klicken Sie auf die Registerkarte *Kompatibilität*. Wählen Sie unter *Kompatibilitätsmodus* das Kontrollkästchen *Programm im Kompatibilitätsmodus ausführen für* und wählen Sie in der Dropdownliste den Modus *Windows Vista (Service Pack 2)*.
5. Wählen Sie das Kontrollkästchen *Desktopgestaltung deaktivieren* und außerdem das Kontrollkästchen *Programm als Administrator ausführen* (Abbildung 5.10). Klicken Sie dann auf *OK*.
6. Klicken Sie *Procexp.exe* mit einem Doppelklick an. Nun sollte sich das Dialogfeld *Benutzerkontensteuerung* öffnen und Sie darauf hinweisen, dass die Anwendung vielleicht Änderungen am Computer vornimmt, gefolgt vom Programmnamen, dem Herausgeber und dem Dateiursprung (Abbildung 5.11). Klicken Sie auf *Ja*.
7. Wenn Sie mit den Lizenzbedingungen einverstanden sind, klicken Sie im Dialogfeld *Process Explorer License Agreement* auf *Agree*. Der Process Explorer lässt sich mit diesen Kompatibilitätseinstellungen aber nicht ausführen. Klicken Sie auf *Schließen*.
8. Klicken Sie *Procexp.exe* mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Klicken Sie auf die Registerkarte *Kompatibilität* und löschen Sie dann die Kontrollkästchen *Programm im Kompatibilitätsmodus ausführen für*, *Desktopgestaltung deaktivieren* und *Programm als Administrator ausführen*. Klicken Sie auf *OK*.
9. Klicken Sie *Procexp.exe* mit der rechten Maustaste an. Klicken Sie auf *Ausführen*, falls sich ein Dialogfeld mit einer Sicherheitswarnung öffnet.

10. Überprüfen Sie, ob die Anwendung einwandfrei arbeitet, und schließen Sie sie dann.

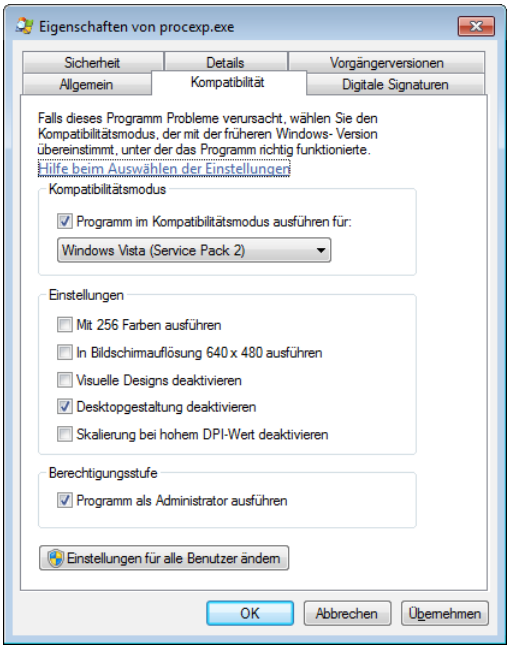


Abbildung 5.10 Konfigurieren der Anwendungskompatibilität

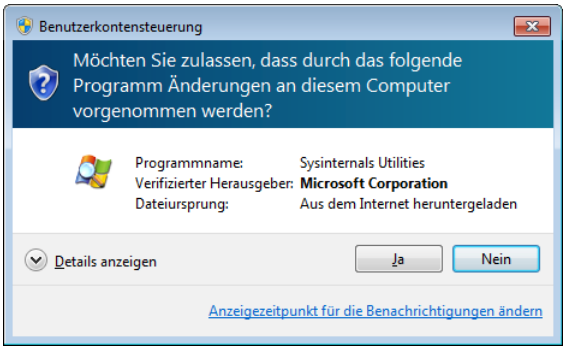

Benutzerkontensteuerung
Möchten Sie zulassen, dass durch das folgende Programm Änderungen an diesem Computer vorgenommen werden?
Programmname: Sysinternals Utilities
Verifizierter Herausgeber: Microsoft Corporation
Dateiursprung: Aus dem Internet heruntergeladen
Details anzeigen
Ja
Nein
Anzeigezeitpunkt für die Benachrichtigungen ändern

Abbildung 5.11 Die Bestätigungsaufforderung der Benutzerkontensteuerung für den Process Explorer

Zusammenfassung der Lektion

- Die häufiger vorkommenden Anwendungskompatibilitätsprobleme können Sie mit der Problembehandlung für Programmkompatibilität diagnostizieren.
- Windows 7 verfügt über mehrere Kompatibilitätsmodi, mit denen es möglich ist, den größten Teil der vorhandenen Software unter Windows 7 zu verwenden.
- Das Application Compatibility Toolkit (ACT) enthält einige Tools, mit denen Sie potenzielle Kompatibilitätsprobleme noch vor der Bereitstellung von Windows 7 in Ihrer Organisation analysieren können.

- Mit dem Compatibility Administrator können Sie nach vorhandenen Kompatibilitätsfixes und Kompatibilitätsmodi suchen, die vielleicht für die betroffenen Anwendungen bereits entwickelt wurden.
- Mit dem Internet Explorer Compatibility Test Tool können Sie Websites und Anwendungen auf Kompatibilitätsprobleme untersuchen, die sich bei der Verwendung von Internet Explorer 8 ergeben könnten.
- Der Windows XP Mode ermöglicht den Einsatz von Anwendungen auf einem virtuellen Computer mit Windows XP. Der Windows XP Mode ist unter Windows 7 Professional, Ultimate oder Enterprise verfügbar.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Anwendungskompatibilität«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie planen, alle Computer in Ihrer Organisation auf Windows 7 Professional umzustellen. Ihre Organisation hat auf den vorhandenen Computern, auf denen Windows XP Professional verwendet wird, mehrere Anwendungen installiert. Wegen Kompatibilitätsproblemen können Sie diese Anwendungen nicht auf Computern installieren, auf denen Windows 7 verwendet wird. Auch mit dem ACT können Sie keinen benutzerdefinierten Kompatibilitätsmodus entwickeln, der sich für diese Anwendungen eignet. Welche der folgenden Lösungen können Sie für die Bereitstellung dieser wichtigen Anwendungen unter Windows 7 verwenden?
   A. Installieren des Windows XP Mode. Anschließend installieren Sie die Anwendungen unter Windows XP.
   B. Erstellen eines benutzerdefinierten Kompatibilitätsfixes für die Anwendung mit dem ACT.
   C. Erstellen eines Shims für die Anwendung mit dem ACT.
   D. Konfigurieren des Kompatibilitätsmodus Windows XP (Service Pack 2) für das Installationsprogramm.
2. Welchen der folgenden Kompatibilitätsmodi würden Sie für eine Anwendung einstellen, die unter Microsoft Windows 2000 Professional funktioniert, aber nicht unter Windows XP?
   A. Windows 98 / Windows Me
   B. Windows NT 4 (Service Pack 5)
   C. Windows XP (Service Pack 2)
   D. Windows 2000

3. Mit welchen der folgenden Dateitypen arbeitet die Problembehandlung für Programmkompatibilität unter Windows 7?
   A. *.cab*-Dateien
   B. *.exe*-Dateien
   C. *.msi*-Dateien
   D. *.zip*-Dateien
4. Eine Anwendung, die in Ihrer Organisation von Administratoren verwendet wird, fordert den Benutzer nicht zur Anhebung der Rechte auf. Welche der folgenden Kompatibilitätsoptionen können Sie für die Anwendung konfigurieren, um sicherzustellen, dass Benutzer mit Administratorrechten immer zur Anhebung der Rechte aufgefordert werden, wenn sie die Anwendung verwenden?
   A. Sie stellen für die Anwendung den Kompatibilitätsmodus Windows XP (Service Pack 3) ein.
   B. Sie aktivieren die Kompatibilitätsoption *Mit 256 Farben ausführen*.
   C. Sie aktivieren die Kompatibilitätsoption *Programm als Administrator ausführen*.
   D. Sie aktivieren die Kompatibilitätsoption *Desktopgestaltung deaktivieren*.
5. Die interne Website Ihrer Organisation wurde bereits vor einigen Jahren entwickelt, als auf allen Clientcomputern Windows XP und Microsoft Internet Explorer 6 verwendet wurden. Sie möchten überprüfen, ob die interne Website nach der Umstellung auf Windows 7 noch richtig angezeigt wird. Mit welchem der folgenden Tools können Sie die Website überprüfen?
   A. Internet Explorer Administration Kit (IEAK)
   B. Application Compatibility Toolkit (ACT)
   C. Windows Automated Installation Kit (Windows AIK, WAIK)
   D. Microsoft Deployment Toolkit (MDT)

Lektion 2: Verwalten von AppLocker und der Richtlinien für Softwareeinschränkung

Gelegentlich ist es erforderlich, genauer festzulegen, welche Anwendungen Benutzer auf einem Computer verwenden können. Vielleicht möchten Sie verhindern, dass bestimmte Anwendungen verwendet werden, oder Sie möchten sicherstellen, dass nur genehmigte Anwendungen im Netzwerk Ihrer Organisation ausgeführt werden können. Unter Windows 7 können Sie die Ausführung von Anwendungen mit zwei verschiedenen Methoden einschränken, nämlich mit AppLocker und mit den Richtlinien für Softwareeinschränkung. Beide werden über Gruppenrichtlinien verwaltet. Mit diesen Methoden können Sie Anwendungen, Installationsdateien, Skripts und sogar DLL-Bibliotheken einschränken. Diese Lektion behandelt die Unterschiede zwischen beiden Technologien und die Situationen, für die sie sich besonders gut eignen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren der Richtlinien für Softwareeinschränkung zur Beschränkung der Ausführung von Anwendungen
- Konfigurieren der AppLocker-Richtlinien zur Beschränkung der Ausführung von Anwendungen, Installationsprogrammen und Skriptdateien

Veranschlagte Zeit für diese Lektion: 50 Minuten

Richtlinien für Softwareeinschränkung

Die *Richtlinien für Softwareeinschränkung* sind nicht nur in Windows 7, sondern auch in Windows XP, Windows Vista, Windows Server 2003 und Windows Server 2008 verfügbar. Verwaltet werden die Richtlinien für Softwareeinschränkung über Gruppenrichtlinien. Sie finden die Richtlinien für Softwareeinschränkung im Knoten *Computerkonfiguration\(Richtlinien\)Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für Softwareeinschränkung* eines Gruppenrichtlinienobjekts (der zusätzliche Knoten *Richtlinien* wird nicht im Editor für lokale Gruppenrichtlinien angezeigt, sondern nur bei der Bearbeitung eines Gruppenrichtlinienobjekts einer Domäne). Wenn Sie die Richtlinien für Softwareeinschränkung verwenden, können Sie die Ausführung einer Anwendung mit der Einstellung *Nicht eingeschränkt* zulassen oder mit der Einstellung *Nicht erlaubt* blockieren.



Hinweis Kontrollieren von Anwendungen durch Berechtigungen

Es ist zwar möglich, die Ausführung einer Anwendung auf der Basis von NTFS-Berechtigungen zu beschränken, aber die Konfiguration der NTFS-Berechtigungen für eine große Zahl von Anwendungen auf einer großen Zahl von Computern bedeutet einen beträchtlichen Verwaltungsaufwand.

Mit den Richtlinien für Softwareeinschränkung können Sie viele der Einschränkungen für Anwendungen festlegen, die sich auch mit AppLocker-Richtlinien festlegen lassen. Gegenüber AppLocker-Richtlinien haben die Richtlinien für Softwareeinschränkung den Vorteil, dass sie sich auch unter Windows XP und Windows Vista anwenden lassen, sowie auf Computern, auf denen Windows 7-Editionen verwendet werden, die AppLocker nicht unterstüt-

zen. Allerdings weisen sie auch den Nachteil auf, dass alle Regeln manuell erstellt werden müssen, weil es keine integrierten Assistenten gibt, die diesen Vorgang unterstützen. Über AppLocker-Richtlinien erfahren Sie mehr im Verlauf dieser Lektion.

Richtlinien für Softwareeinschränkung werden in einer bestimmten Reihenfolge angewendet, wobei die spezielleren Regeln Vorrang vor den allgemeineren haben. Die Reihenfolge von der speziellsten Regel (Hash) bis zur allgemeinsten (Standard) ist wie folgt:

1. Hashregeln
2. Zertifikatregeln
3. Pfadregeln
4. Netzwerkzonenregeln
5. Standardregeln

Werden für dasselbe Programm zwei widersprüchliche Regeln mit derselben Sicherheitsstufe eingerichtet, hat die speziellere Regel Vorrang. Eine Hashregel, die eine bestimmte Anwendung unbeschränkt zulässt, hat zum Beispiel Vorrang vor einer Pfadregel, die diese Anwendung blockiert. Die AppLocker-Richtlinien wirken anders, denn dort gibt es keine Rangordnung in den Regeln, aber eine Blockierungsregel hat in AppLocker immer Vorrang vor einer Zulassungsregel.



Hinweis AppLocker setzt die Richtlinien für Softwareeinschränkung außer Kraft

In Umgebungen, in denen die Richtlinien für Softwareeinschränkung und AppLocker beide verwendet werden, haben die AppLocker-Richtlinien Vorrang. Wenn es eine AppLocker-Richtlinie gibt, die eine bestimmte Anwendung zulässt, die von den Richtlinien für Softwareeinschränkung blockiert wird, lässt sich die Anwendung ausführen.

Sicherheitsstufen und Standardregeln

Der Knoten *Sicherheitsstufen* ermöglicht die Erstellung einer Standardregel für die Richtlinien für Softwareeinschränkung. Die Standardregel gilt dann, wenn keine andere Richtlinie für Softwareeinschränkung zu einer Anwendung passt. Es kann immer nur eine Standardregel aktiviert sein. Die in Abbildung 5.12 gezeigten drei Standardregeln sind:

- **Nicht erlaubt** Wenn diese Regel aktiviert ist, können Benutzer keine Anwendung ausführen, deren Ausführung nicht durch eine Richtlinie für Softwareeinschränkung zugelassen wird.
- **Standardbenutzer** Wenn diese Regel aktiviert ist, können Benutzer Anwendungen ausführen, solange für diese Anwendungen keine Administratorrechte erforderlich sind. Benutzer können nur dann Anwendungen verwenden, die Administratorrechte erfordern, wenn eine Zulassungsregel für diese Anwendungen erstellt wurde.
- **Nicht eingeschränkt** Wird diese Regel als Standardregel aktiviert, kann ein Benutzer eine Anwendung verwenden, solange diese Anwendung nicht durch eine Richtlinie für Softwareeinschränkung blockiert wird.

Wenn Sie eine Zulassungsliste für Anwendungen erstellen möchten, werden Sie wahrscheinlich die Blockierungsregel aktivieren. Dadurch ist sichergestellt, dass keine Anwendung ausgeführt werden kann, die nicht ausdrücklich zugelassen wurde. Wenn Sie nur einige problematische Anwendungen sperren möchten, aber nicht für jede in Ihrer Umgebung

verwendete Anwendung eine Regel erstellen möchten, sollten Sie die Standardregel *Nicht eingeschränkt* aktivieren. Dann können alle Anwendungen ausgeführt werden, die Sie nicht explizit blockieren.

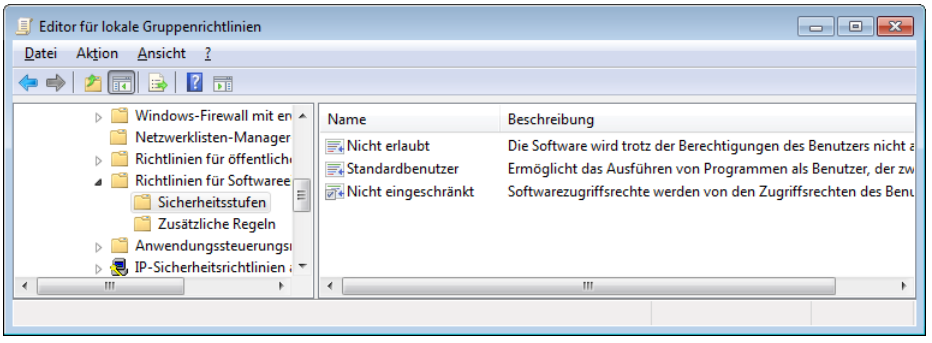


Abbildung 5.12 Die Standardregeln der Richtlinien für Softwareeinschränkung

Erzwingen

Mit der Richtlinie *Erzwingen* (Abbildung 5.13) können Sie festlegen, ob die Richtlinien für Softwareeinschränkung für alle Softwaredateien außer Bibliotheken (beispielswiese DLLs) gelten, oder für alle Softwaredateien (einschließlich DLLs). Wenn die Standardsicherheitsstufe *Nicht erlaubt* eingestellt ist und Sie die Erzwingungsrichtlinien so einstellen, dass sie für alle Softwaredateien gelten, müssen Sie für alle DLLs, die von einem Programm verwendet werden, Regeln konfigurieren, damit Sie das Programm verwenden können. Microsoft empfiehlt, keine DLLs einzubeziehen, sofern Sie keine Computer aus einer Hochsicherheitsumgebung verwalten. Die Verwaltung von Regeln für DLLs bedeutet nämlich eine beträchtliche Arbeitsbelastung für den Administrator, der die Richtlinien für Softwareeinschränkung verwalten muss.

Sie können die Erzwingungsrichtlinie verwenden, um die Richtlinien für Softwareeinschränkung für alle Benutzer vorzuschreiben, oder für alle Benutzer mit Ausnahme der lokalen Administratoren. Außerdem können Sie mit dieser Richtlinie festlegen, ob Zertifikatregeln durchgesetzt oder ignoriert werden. Der Nachteil der Erzwingung der Zertifikatregeln besteht in dem erforderlichen Aufwand, durch den die Leistung eines Computers deutlich sinken kann.

Designierte Dateitypen

Mit der Richtlinie *Designierte Dateitypen* (Abbildung 5.14) können Sie festlegen, welche Erweiterungen als Dateinamenserweiterungen von ausführbaren Dateien eingestuft werden sollen, für die somit die Richtlinien für Softwareeinschränkung gelten. Mit den Schaltflächen *Hinzufügen* und *Entfernen* können Administratoren die Liste der Erweiterungen ändern, die unter die Richtlinien für Softwareeinschränkung fallen. Die Standarderweiterungen für ausführbare Dateien wie *.com*, *.exe* und *.vbs* lassen sich allerdings nicht auf diese Weise entfernen, diese Erweiterungen werden immer als Namenserweiterungen von ausführbaren Dateien eingestuft.

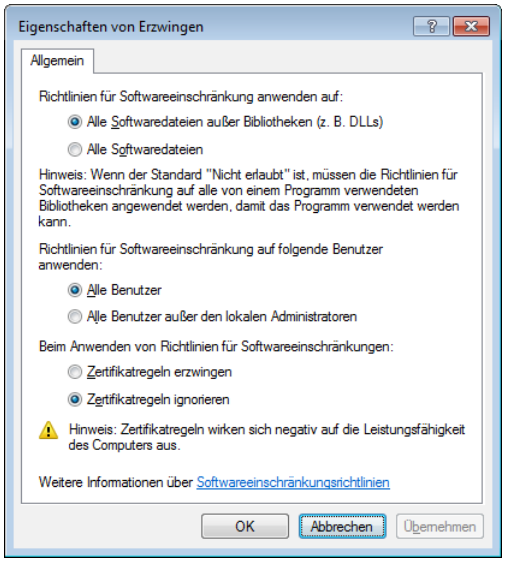

Eigenschaften von Erzwingen
Allgemein
Richtlinien für Softwareeinschränkung anwenden auf:
Alle Softwaredateien außer Bibliotheken (z. B. DLLs)
Alle Softwaredateien
Hinweis: Wenn der Standard "Nicht erlaubt" ist, müssen die Richtlinien für Softwareeinschränkung auf alle von einem Programm verwendeten Bibliotheken angewendet werden, damit das Programm verwendet werden kann.
Richtlinien für Softwareeinschränkung auf folgende Benutzer anwenden:
Alle Benutzer
Alle Benutzer außer den lokalen Administratoren
Beim Anwenden von Richtlinien für Softwareeinschränkungen:
Zertifikatregeln erzwingen
Zertifikatregeln ignorieren
Hinweis: Zertifikatregeln wirken sich negativ auf die Leistungsfähigkeit des Computers aus.
Weitere Informationen über Softwareeinschränkungsrichtlinien
OK
Abbrechen
Übernehmen

Abbildung 5.13 Die Erzwingungsrichtlinie der Richtlinien für Softwareeinschränkung

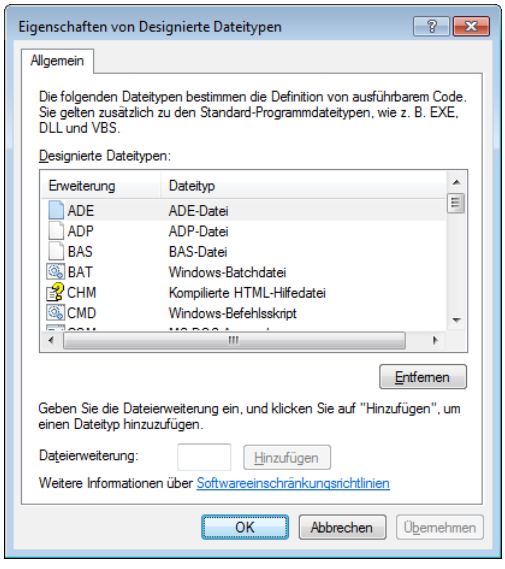


Abbildung 5.14 Designierte Dateitypen

Pfadregeln

Pfadregeln ermöglichen die Angabe einer Datei, eines Ordners oder eines Registrierungsschlüssels als Ziel einer Richtlinie für Softwareeinschränkung (Abbildung 5.15). Je spezieller eine Pfadregel ist, desto höher ist ihre Vorrangstufe. Gibt es zum Beispiel eine Pfadregel, die die Datei *C:\Program Files\Anwendung\Anwendung.exe* auf *Nicht eingeschränkt* einstellt, und eine zweite, die den Ordner *C:\Program Files\Anwendung* auf *Nicht erlaubt* einstellt, hat die speziellere Pfadregel Vorrang und die Anwendung kann ausgeführt werden. In Pfad-

regeln dürfen auch Platzhalter verwendet werden. Daher lässt sich beispielsweise eine Pfadregel für *C:\Program Files\Anwendung*.exe* festlegen. Regeln mit Platzhalter sind allgemeiner (weniger speziell) als Regeln, in denen der vollständige Pfadname einer Datei angegeben wird.

Pfadregeln haben allerdings den Nachteil, dass sie von bestimmten Speicherorten für Dateien und Ordnern ausgehen. Wenn Sie zum Beispiel eine Pfadregel für die Sperrung der Anwendung *C:\Anwendungen\Dateiaustausch.exe* erstellen, könnte ein Angreifer dieselbe Anwendung ausführen, indem er sie in einen anderen Ordner verschiebt oder ihr einen anderen Namen gibt. Pfadregeln funktionieren nur dann, wenn die Berechtigungen von Dateien und Ordnern im zugrunde liegenden Dateisystem das Umbenennen oder Verschieben von Dateien nicht zulassen.

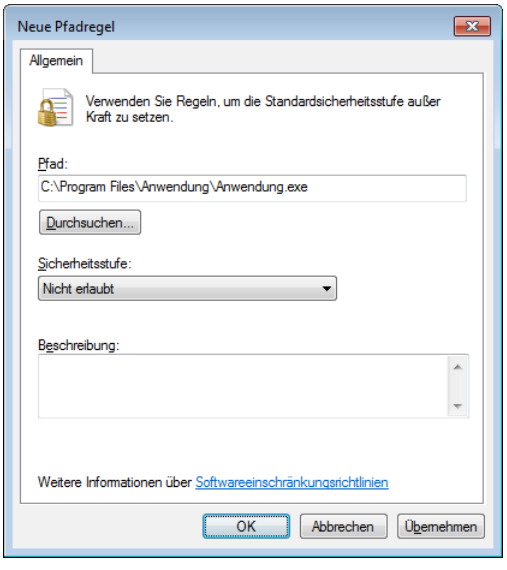


Abbildung 5.15 Eine Pfadregel für die Richtlinien für Softwareeinschränkung

Hashregeln

Hashregeln verwenden einen digitalen Fingerabdruck, der eine Datei auf der Basis ihrer binären Eigenschaften identifiziert (Abbildung 5.16). Das bedeutet, dass sich eine Datei, für die Sie eine Hashregel erstellt haben, auch dann identifizieren lässt, wenn sie umbenannt wurde oder an einem anderen Ort gespeichert ist. Hashregeln funktionieren mit jeder Datei und setzen keine digitale Signatur der Datei voraus. Der Nachteil der Hashregeln besteht darin, dass sie auf Dateibasis erstellt werden müssen. Sie können Hashregeln für die Richtlinien für Softwareeinschränkung nicht automatisch erstellen. Sie müssen jede einzelne Regel manuell erstellen. Außerdem müssen Sie eine Hashregel jedes Mal aktualisieren, wenn Sie ein Update auf die Datei anwenden, für die die Hashregel gilt. Softwareupdates ändern die binären Eigenschaften einer Datei. Das bedeutet, dass der digitale Fingerabdruck nicht mehr zu der durch das Update geänderten Datei passt.

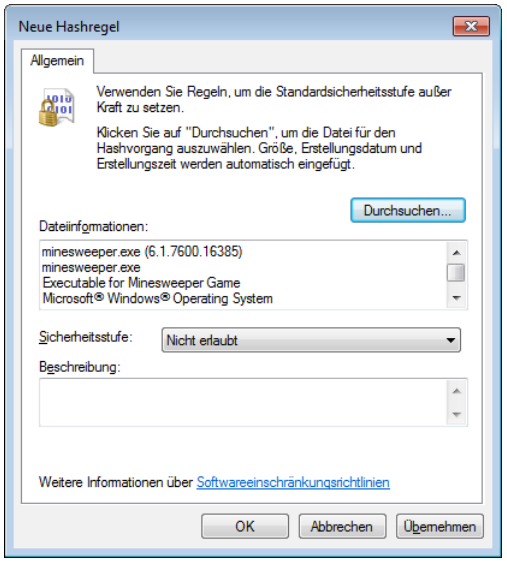


Abbildung 5.16 Eine Hashregel für Minesweeper

Zertifikatregeln

Zertifikatregeln verwenden ein Zertifikat des Herausgebers, um Anwendungen zu identifizieren, die von diesem Herausgeber signiert wurden. Eine einzige Zertifikatregel kann für mehrere Anwendungen gelten und dabei so sicher wie eine Hashregel sein. Es ist nicht nötig, eine Zertifikatregel zu ändern, wenn der Hersteller ein Softwareupdate veröffentlicht, weil die aktualisierte Anwendung weiterhin mit dem Zertifikat des Herstellers signiert ist. Wenn Sie eine Zertifikatregel konfigurieren möchten, müssen Sie sich ein Zertifikat des Herstellers beschaffen. Zertifikatregeln bedeuten für die Computer, auf denen sie angewendet werden, einen gewissen Rechenaufwand, weil die Gültigkeit eines Zertifikats überprüft werden muss, bevor die Anwendung ausgeführt werden kann. Ein weiterer Nachteil der Zertifikatregeln besteht darin, dass sie für alle Anwendungen eines Herstellers gelten. Wenn sie von einem bestimmten Hersteller, der 20 Anwendungen im Lieferprogramm hat, nur eine Anwendung zulassen möchten, sind Sie mit einer anderen Art von Richtlinien für Softwareeinschränkung besser beraten, denn wenn Sie eine Zertifikatregel einrichten, können die Benutzer auch jede andere der 20 Anwendungen verwenden.

Netzwerkzonenregeln

Die Internet-Zonenregeln gelten nur für Windows Installer-Pakete (*.msi*), die mit dem Internet Explorer heruntergeladen wurden. Netzwerkzonenregeln gelten nur für *.msi*-Dateien und nicht für andere Anwendungen, beispielsweise für *.exe*-Dateien, die mit dem Internet Explorer beschafft wurden. Netzwerkzonenregeln unterscheiden Installer-Pakete nach den Websites, von denen sie heruntergeladen wurden. Die potenziellen Orte sind *Internet*, *Lokales Intranet*, *Eingeschränkte Sites*, *Vertrauenswürdige Sites* und *Lokaler Computer*.



Weitere Informationen Richtlinien für Softwareeinschränkung

Weitere Informationen über die Richtlinien für Softwareeinschränkung erhalten Sie im Microsoft TechNet unter *http://technet.microsoft.com/en-us/library/cc782792(WS.10).aspx*.

Schnelltest

- Welchen Vorteil hat eine Hashregel gegenüber einer Pfadregel?

Antwort zum Schnelltest

- Hashregeln sind wie digitale Fingerabdrücke, die eine bestimmte Datei identifizieren. Eine Pfadregel funktioniert nur auf der Basis eines Dateinamens und eines Pfads. Das bedeutet, dass Malware an Orten eingefügt werden kann, die von Pfadregeln zugelassen werden, und dort ausgeführt werden kann.

AppLocker-Anwendungssteuerungsrichtlinien

AppLocker wurde mit Windows 7 eingeführt und ist nur in den Editionen Enterprise und Ultimate verfügbar. *AppLocker-Richtlinien* lassen sich mit den Richtlinien für Softwareeinschränkung vergleichen, haben aber einige Vorteile. Sie lassen sich zum Beispiel auf bestimmte Benutzer- oder Gruppenkonten anwenden und können auch für alle zukünftigen Versionen eines Produkts gelten. Wie Sie in diesem Kapitel bereits erfahren haben, gelten Hashregeln nur für eine bestimmte Version einer Anwendung und müssen nach jedem Update der Anwendung neu berechnet werden. Sie finden die AppLocker-Richtlinien im Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Anwendungssteuerungsrichtlinien* eines Standardgruppenrichtlinienobjekts von Windows 7 oder Windows Server 2008 R2.

AppLocker ist darauf angewiesen, dass der Dienst *Anwendungsidentität* läuft. Nach der Installation von Windows 7 ist der Starttyp dieses Dienstes auf *Manuell* eingestellt. Beim Test von AppLocker sollten Sie den Starttyp für den Fall, dass Sie Regeln falsch konfigurieren, auf *Manuell* eingestellt lassen. Dann starten Sie den Computer neu und die AppLocker-Regeln sind nicht mehr wirksam. Erst wenn Sie sicher sind, dass die Regeln alle korrekt sind, sollten Sie den Starttyp des Dienstes *Anwendungsidentität* auf *Automatisch* stellen. Testen Sie die AppLocker-Regeln sehr sorgfältig, denn es ist durchaus möglich, einen Windows 7-Computer so zu blockieren, dass er unbrauchbar wird. AppLocker-Richtlinien werden auch Anwendungssteuerungsrichtlinien genannt.

Standardregeln

Standardregeln sind Regeln, die automatisch erstellt werden können und Benutzern den Zugriff auf Windows- und Programmdateien ermöglichen. Standardregeln sind erforderlich, weil AppLocker über eine vordefinierte Blockierungsgrundregel (fallback block rule) verfügt, die alle Anwendungen blockiert, die nicht von einer Zulassungsregel zugelassen werden. Das bedeutet, dass Sie nach der Aktivierung von AppLocker keine Anwendung, kein Skript und kein Installationsprogramm ausführen können, für das es keine Zulassungsregel gibt. Für jeden Regeltyp gibt es andere Standardregeln. Die Standardregeln sind sehr allgemein formuliert und können von Administratoren an die vorliegende Umgebung angepasst werden. Bei den Standardregeln für Anwendungen handelt es sich zum Beispiel um Pfadregeln. Wer als Administrator eine höhere Sicherheit erreichen möchte, könnte diese Standardregeln durch Herausgeber- oder Hashregeln ersetzen.

Sie können Standardregeln erstellen, indem Sie den Knoten *Ausführbare Regeln*, *Windows Installer-Regeln* oder *Skriptregeln* mit der rechten Maustaste anklicken und dann auf *Standardregeln erstellen* klicken. Abbildung 5.17 zeigt die Standardregeln unter dem Knoten *Ausführbare Regeln*.

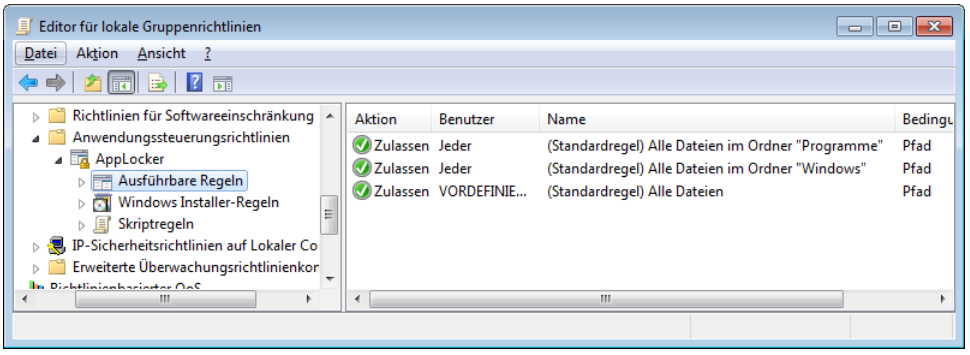


Abbildung 5.17 Standardregeln für ausführbare Dateien

Blockierungsregeln

Sie können AppLocker-Regeln festlegen, die Anwendungen blockieren oder zulassen. Explizit definierte *Blockierungsregeln* haben Vorrang vor allen Zulassungsregeln, unabhängig davon, wie die Regel definiert ist. Darin unterscheiden sich AppLocker-Regeln von den Richtlinien für Softwareeinschränkung, wo ein Regeltyp Vorrang vor einem anderen haben kann. Die bereits erwähnte Blockierungsgrundregel hat vor keiner Regel Vorrang. Die Blockierungsgrundregel beschränkt einfach nur die Ausführung von Anwendungen, die nicht ausdrücklich zugelassen wurden. Eine Blockierungsregel brauchen Sie nur hinzuzufügen, wenn eine andere AppLocker-Regel die Ausführung einer Anwendung, einer Installationsdatei oder eines Skripts zulässt. Nehmen wir zum Beispiel an, Sie möchten jedem Mitarbeiter Ihrer Organisation mit Ausnahme der Mitarbeiter in der Gruppe *Accounting* die Verwendung einer Anwendung namens *Alpha.exe* ermöglichen. Dann müssen Sie zwei Regeln erstellen. Die erste Regel erlaubt jedem, *Alpha.exe* zu verwenden. Die zweite blockiert *Alpha.exe* für die Gruppe *Accounting*. AppLocker-Regeln lassen zwar Ausnahmen zu, aber nicht auf der Basis der Gruppenmitgliedschaft.

Mit explizit definierten Blockierungsregeln können Sie die Ausführung von Anwendungen verhindern, die durch die Standardregeln zugelassen werden. Die Standardregeln erlauben auf einem Windows 7-Computer zum Beispiel die Ausführung der Anwendung *Solitaire.exe*. Mit einer expliziten Blockierungsregel können Sie die Verwendung von Solitär verhindern. Sie können die Ausführung von Solitär auch mit einer Ausnahme in den Standardregeln verhindern. Ausnahmen werden im Verlauf dieser Lektion noch besprochen.

Ausführbare Regeln (Regeln für ausführbare Dateien)

Ausführbare Regeln wirken auf Dateien mit den Namenserweiterungen *.exe* und *.com*, also auf ausführbare Dateien. AppLocker-Richtlinien werden hauptsächlich für ausführbare Dateien erstellt und es ist sehr wahrscheinlich, dass der größte Teil der AppLocker-Richtlinien, mit denen Sie es in Ihrer Organisation zu tun haben, zu den ausführbaren Regeln gehört. Die ausführbaren Standardregeln sind Pfadregeln, die jedem die Ausführung aller Anwendungen aus den Ordnern *Programme* und *Windows* ermöglichen. Außerdem erlauben

die Standardregeln den Mitgliedern der Gruppe *Administratoren* die Ausführung aller Anwendungen, die auf dem Computer installiert sind. Die Standardregeln oder Regeln, die wie die Standardregeln wirken, sind wichtig, weil Windows nicht richtig funktioniert, wenn bestimmte Anwendungen, die von den Standardregeln zugelassen werden, nicht ausgeführt werden dürfen. Bei der Erstellung einer Regel wird als Benutzer oder Gruppe *Jeder* vorgegeben (Abbildung 5.18), auch wenn es gar keine lokale Gruppe namens *Jeder* gibt. Wenn Sie die Regel ändern möchten, können Sie eine andere Sicherheitsgruppe oder ein Benutzerkonto angeben.

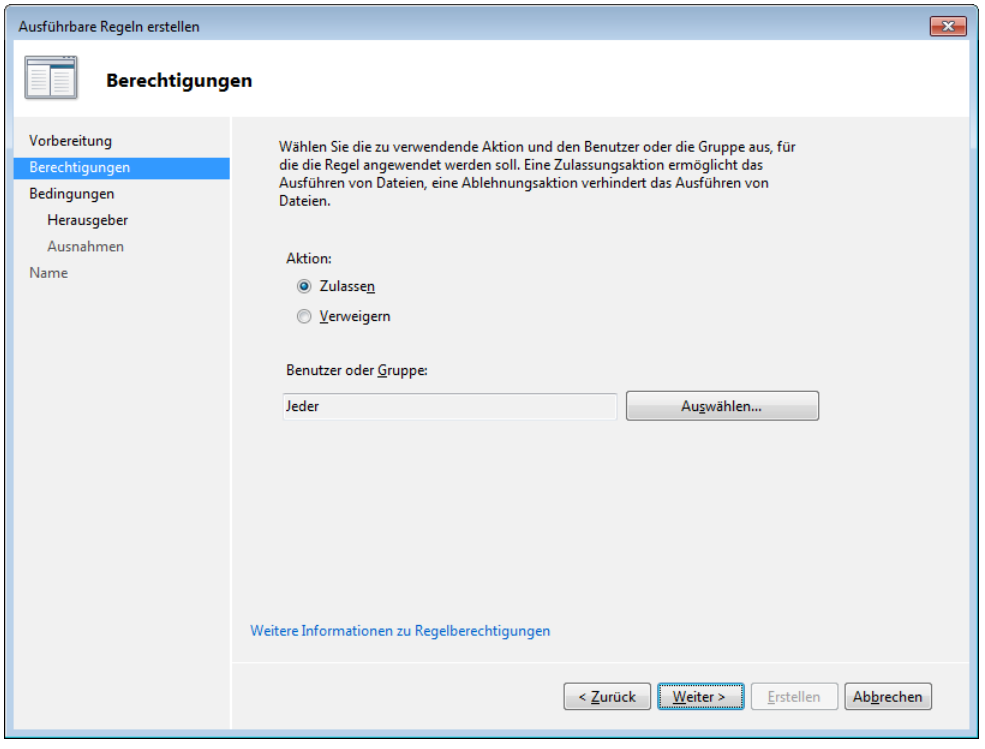


Abbildung 5.18 Der vorgegebene Gültigkeitsbereich einer Standardregel

Windows Installer-Regeln

Windows Installer-Regeln gelten für Dateien mit den Namenserweiterungen *.msi* und *.msp*. Sie können Installer-Regeln verwenden, um die Installation von Software auf Computern zuzulassen oder zu sperren. Die Windows Installer-Standardregeln erlauben der Gruppe *Jeder* die Verwendung aller digital signierten Windows Installer-Dateien und aller Windows Installer-Dateien aus dem Verzeichnis *%SystemDrive%\Windows\Installer*, sowie Mitgliedern der lokalen Gruppe *Administratoren* die Ausführung aller *.msi*- oder *.msp*-Dateien. Die Standardregeln lassen die Installation von Software und Softwareupdates über Gruppenrichtlinien zu.

Auch wenn eine AppLocker-Regel jedem den Zugang zu einer bestimmten Installationsdatei ermöglicht, ist zur Installation der Software trotzdem noch die entsprechende Berechtigung erforderlich. Installer-Regeln sind besonders dann von Nutzen, wenn Ihre Organisation über

portable Computer verfügt, auf denen Windows 7 verwendet wird, und die es erforderlich machen, Benutzern die Rechte eines lokalen Administrators zu geben. Nach der Entfernung der Standardregel, die lokalen Administratoren die Verwendung beliebiger Installer-Dateien erlaubt, müssen Sie außerdem den Zugang zum Editor für lokale Gruppenrichtlinien beschränken, damit lokale Administratoren diese Richtlinieneinstellung nicht ändern können.

Skriptregeln

Skriptregeln wirken auf Dateien mit den Namenserweiterungen *.ps1*, *.bat*, *.cmd*, *.vbs* und *.js*. Es ist zwar möglich, für Skripts Herausgeberregeln festzulegen, aber die meisten Skripts werden von Administratoren kurzfristig nach Bedarf erstellt und nur selten digital signiert. Für Skripts, die nur selten geändert werden, sollten Sie Hashregeln verwenden und Pfadregeln für Ordner erstellen, in denen Skripts gespeichert sind, die häufig geändert werden. Wenn Sie Pfadregeln erstellen, sollen Sie dafür sorgen, dass die Berechtigungen für die Ordner, in denen die Skripts gespeichert werden, so eingestellt sind, dass dort nichtautorisierte Personen nicht heimlich unerwünschte Skripts speichern können. Die Standardskriptregeln lassen die Ausführung aller Skripts zu, die in den Ordnern *Programme* und *Windows* gespeichert sind. Außerdem erlauben die Standardskriptregeln den Mitgliedern der vordefinierten Gruppe *Administratoren* die Ausführung aller Skripts, unabhängig von dem Ort, an dem sie gespeichert sind.

DLL-Regeln

DLL-Regeln wirken auf Bibliotheksdateien mit den Namenserweiterungen *.dll* und *.ocx*. Bibliotheken unterstützen die Ausführung von Anwendungen. DLL-Regeln werden bei der Aktivierung von AppLocker nicht automatisch aktiviert. DLL-Regeln bieten ein Höchstmaß an Sicherheit, allerdings auf Kosten der Leistung. Sie müssen für jede DLL, die von einer Anwendung auf Ihrem Windows 7-Clientcomputer verwendet wird, eine DLL-Regel erstellen. Die Erstellung der Regeln lässt sich zwar in gewissem Umfang automatisieren und wird dadurch einfacher, aber Benutzer können eine gewisse Verzögerung feststellen, weil AppLocker jede DLL, die von einer Anwendung geladen wird, bei jedem Ladevorgang überprüfen muss. Zur Aktivierung der DLL-Regeln klicken Sie in einem Gruppenrichtlinieneditor den Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Anwendungssteuerungsrichtlinien\AppLocker* mit der rechten Maustaste an, wählen die Registerkarte *Erweitert* und markieren dann das Kontrollkästchen *DLL-Regelsammlung aktivieren* (Abbildung 5.19).

Herausgeberregeln

Die *Herausgeberregeln* von AppLocker überprüfen Dateien auf der Basis des Codesignaturzertifikats, das der Herausgeber der Datei verwendet hat. Anders als bei einer Zertifikatregel der Richtlinien für Softwareeinschränkung ist es nicht erforderlich, für die Herausgeberregel ein Zertifikat zu beschaffen, weil die Details der digitalen Signatur aus einer Referenzanwendungsdatei ausgelesen werden. Wenn eine Datei nicht digital signiert ist, können Sie keine AppLocker-Herausgeberregel für die Datei erstellen.

Herausgeberregeln sind flexibler als Hashregeln, weil sie nicht nur für eine bestimmte Dateiversion gelten, sondern auch für alle zukünftigen Versionen der Datei gelten können. Das bedeutet, dass Sie die Herausgeberregel nicht nach jeder Aktualisierung der Software neu erstellen müssen, weil die vorhandene Regel noch gilt. Mit der Einstellung *Genau* können Sie die Regel auch auf eine bestimmte Dateiversion einschränken (Abbildung 5.20).

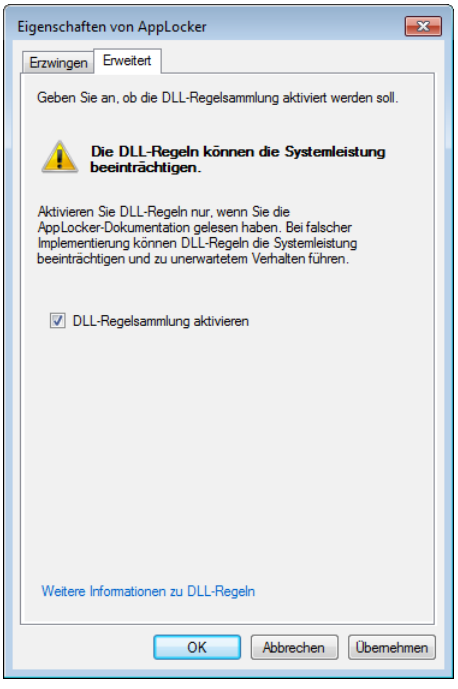

Eigenschaften von AppLocker
Erzwingen
Erweitert
Geben Sie an, ob die DLL-Regelsammlung aktiviert werden soll.
Die DLL-Regeln können die Systemleistung beeinträchtigen.
Aktivieren Sie DLL-Regeln nur, wenn Sie die AppLocker-Dokumentation gelesen haben. Bei falscher Implementierung können DLL-Regeln die Systemleistung beeinträchtigen und zu unerwartetem Verhalten führen.
DLL-Regelsammlung aktivieren
Weitere Informationen zu DLL-Regeln
OK
Abbrechen
Übernehmen

Abbildung 5.19 Aktivieren der DLL-Regelsammlung

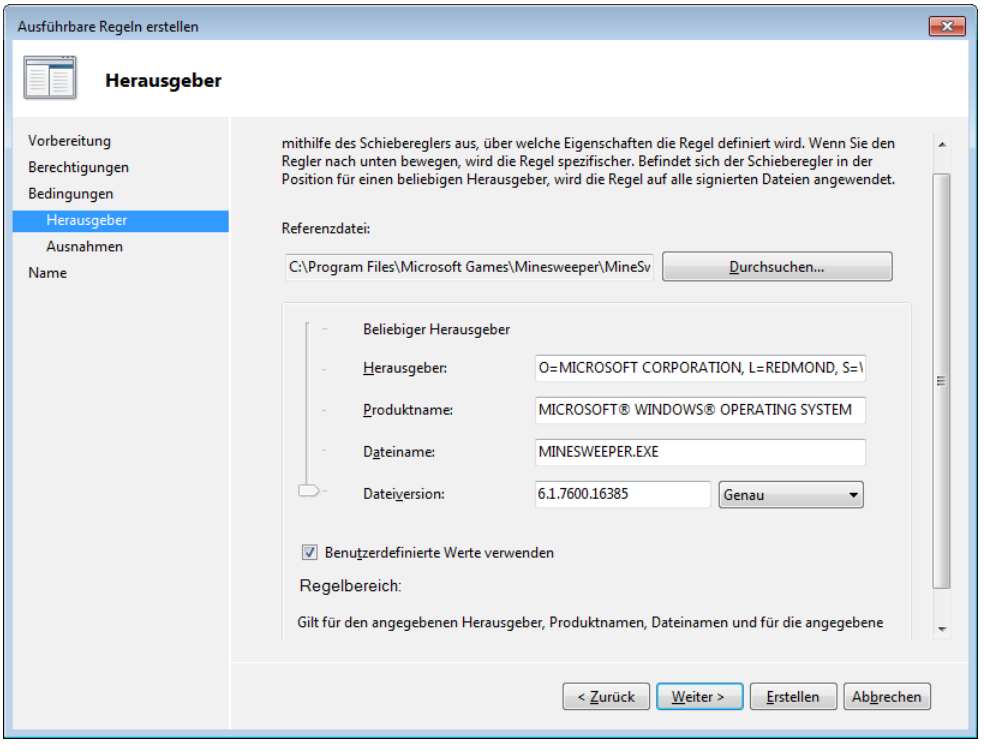


Abbildung 5.20 AppLocker-Herausgeberregel

Mit dem Schieberegler können Sie den Gültigkeitsbereich der Herausgeberregel ändern, damit sie für einen bestimmten, vom Herausgeber signierten Dateinamen gilt, für ein bestimmtes, vom Herausgeber signiertes Produkt, für jedes vom Herausgeber signierte Produkt oder für jedes signierte Produkt eines beliebigen Herausgebers. Diese letzte Einstellung gilt aber nicht für beliebige Anwendungen, sondern nur für Anwendungen, die von den Herausgebern digital signiert wurden. Wenn Sie eine Zulassungsregel mit der Einstellung *Beliebiger Herausgeber* erstellen, können alle Anwendungen ausgeführt werden, die von ihren Herausgebern signiert wurden. Aber Anwendungen, die nicht signiert sind, werden dann von der Regel blockiert.

Hashregeln

Hashregeln funktionieren in AppLocker im Prinzip so wie in den Richtlinien für Softwareeinschränkung. Hashregeln ermöglichen die Identifikation einer bestimmten binären Datei mit einem digitalen Fingerabdruck, auch wenn die Datei nicht digital signiert ist. Dieser »Fingerabdruck« ist eigentlich ein Hashwert, der für die Datei berechnet wird. In AppLocker lassen sich Dateihashwerte einfacher als in den Richtlinien für Softwareeinschränkung verwalten, weil sich die Erstellung der Dateihashwerte für Dateien, die an einem bestimmten Ort gespeichert sind, mit dem Regelerstellungsassistenten automatisieren lässt. Wie bereits erwähnt, haben Hashregeln den Nachteil, dass der Dateihashwert nach jeder Aktualisierung der Datei neu berechnet werden muss, weil der digitale Fingerabdruck (der alte Hashwert) durch die Änderung der Datei ungültig wird. Zur Berechnung des Hashwerts suchen Sie die Datei im Assistenten heraus. Es ist auch möglich, einen Ordner auszuwählen und für alle Dateien aus diesem Ordner die entsprechenden Hashwerte zu berechnen. Dabei werden jedoch die Dateien nicht berücksichtigt, die sich in Unterordnern des ausgewählten Ordners befinden. Abbildung 5.21 zeigt eine Dateihashregel. Ausnahmen lassen sich für Dateihashregeln nicht festlegen, weil ein Dateihashwert sowieso nur für eine ganz bestimmte Datei gilt.

Pfadregeln

AppLocker-*Pfadregeln* funktionieren so ähnlich wie die Pfadregeln der Richtlinien für Softwareeinschränkung, die in dieser Lektion bereits besprochen wurden. In Pfadregeln können Sie den Pfad eines Ordners angeben, wodurch die Pfadregel für den gesamten Inhalt des Ordners einschließlich seiner Unterordner gilt, oder den Pfadnamen einer bestimmten Datei. Der Vorteil der Pfadregeln liegt darin, dass sie einfach zu erstellen sind. Allerdings haben sie auch den Nachteil, die unsicherste Form der AppLocker-Regeln zu sein. Ein Angreifer kann eine Pfadregel nutzen, indem er eine ausführbare Datei in einen Ordner kopiert, für den eine Zulassungsregel gilt, oder indem er eine bestimmte Datei überschreibt, die durch eine Pfadregel zugelassen wird. Pfadregeln sind nur so sicher wie die Berechtigungen für Dateien und Ordner, die auf dem Computer gelten. Abbildung 5.22 zeigt eine AppLocker-Pfadregel.

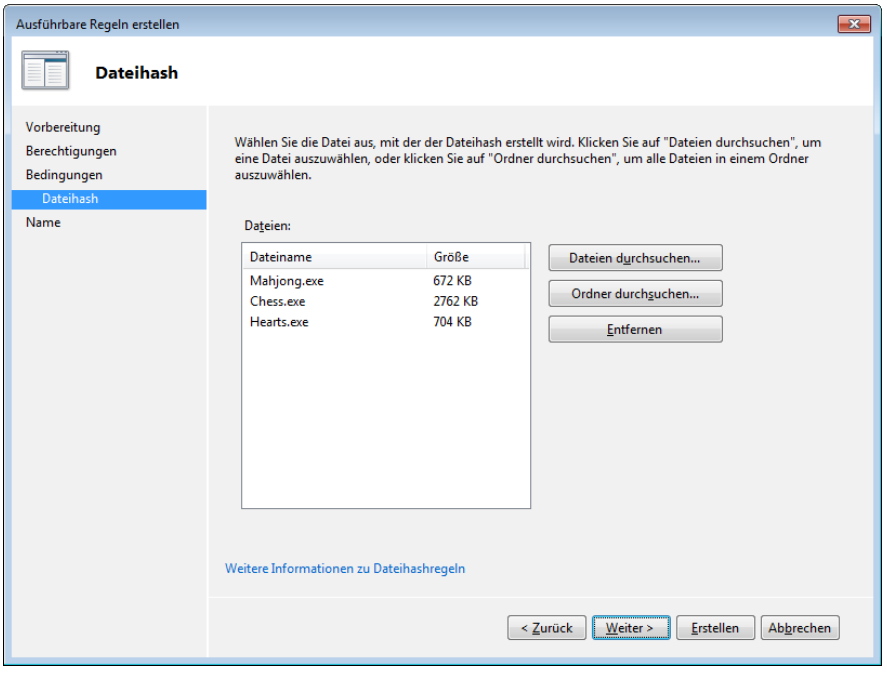


Abbildung 5.21 AppLocker-Dateihashregel

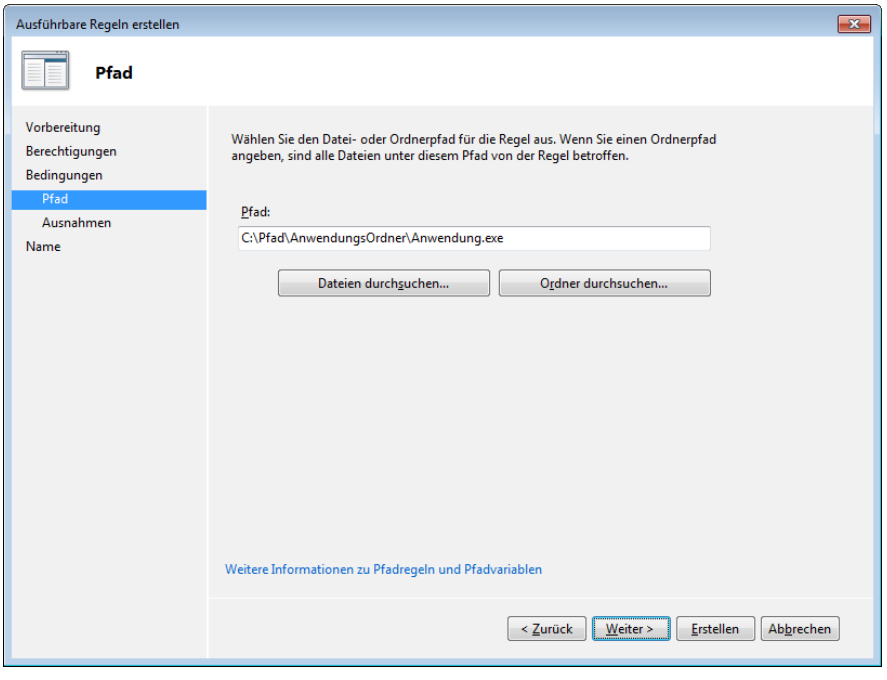


Abbildung 5.22 Eine AppLocker-Pfadregel

Automatisches Erstellen von Regeln

AppLocker weist gegenüber den Richtlinien für Softwareeinschränkung den wichtigen Vorteil auf, dass sich Regeln automatisch generieren lassen. Zur Konfiguration von AppLocker-Regeln können Sie den Knoten *Ausführbare Regeln*, *Windows Installer-Regeln* oder *Skriptregeln* mit der rechten Maustaste anklicken und dann auf *Regeln automatisch generieren* klicken. Sie werden zur Angabe eines Ordners aufgefordert, den der Assistent durchsuchen soll. Auf der nächsten Seite können Sie zum Beispiel festlegen, ob der Assistent automatisch Herausgeberregeln für digital signierte Dateien erstellen soll und ob er für eine nichtsignierte Datei eine Hashregel oder eine Pfadregel erstellen soll (Abbildung 5.23). Sie können den Assistenten auch anweisen, für alle Dateien des Typs, den Sie konfigurieren, eine Dateihashregel zu erstellen. Der Assistent zur automatischen Erstellung von Regeln untersucht bei der Erstellung der Regeln den angegebenen Ordner und alle darin enthaltenen Unterordner.

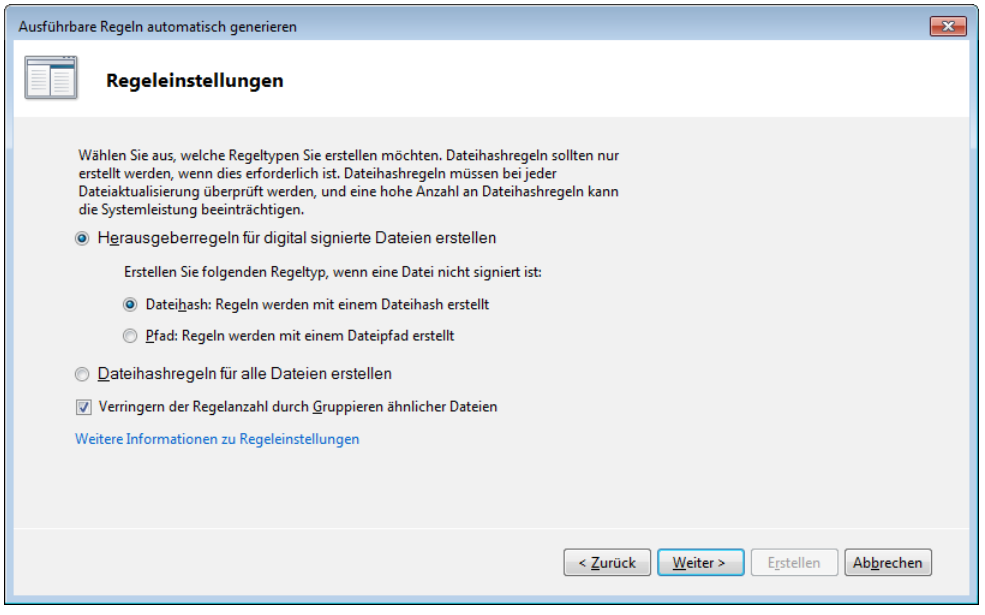

Ausführbare Regeln automatisch generieren
Regeleinstellungen
Wählen Sie aus, welche Regeltypen Sie erstellen möchten. Dateihashregeln sollten nur erstellt werden, wenn dies erforderlich ist. Dateihashregeln müssen bei jeder Dateiaktualisierung überprüft werden, und eine hohe Anzahl an Dateihashregeln kann die Systemleistung beeinträchtigen.
Herausgeberregeln für digital signierte Dateien erstellen
Erstellen Sie folgenden Regeltyp, wenn eine Datei nicht signiert ist:
Dateihash: Regeln werden mit einem Dateihash erstellt
Pfad: Regeln werden mit einem Dateipfad erstellt
Dateihashregeln für alle Dateien erstellen
Verringern der Regelanzahl durch Gruppieren ähnlicher Dateien
Weitere Informationen zu Regeleinstellungen
< Zurück
Weiter >
Erstellen
Abbrechen

Abbildung 5.23 Automatisches Generieren von Regeln

Konfigurieren von Ausnahmen

Mit Ausnahmen lassen sich bestimmte Anwendungen von der Wirkung allgemeiner formulierter Regeln ausnehmen. Beispielsweise können Sie eine Herausgeberregel erstellen, die alle Versionen einer Anwendung namens Alpha von Contoso zulässt, und dann eine Ausnahme festlegen, mit der die Ausführung der Version 42 der Anwendung Alpha gesperrt wird. Sie können unabhängig von der Art der Regel, die Sie erstellen, jede verfügbare Methode verwenden, um eine Ausnahme zu definieren. Wie Abbildung 5.24 zeigt, können Sie zum Beispiel eine Herausgeberregel erstellen, die alle von Microsoft herausgegebenen Anwendungen zulässt, und dann mit einem Dateihash eine Ausnahme für *Solitaire.exe* definieren. Diese Beispielregel funktioniert natürlich nur, wenn keine Standardpfadregel für den Ordner *Programme* erstellt wird. Ausnahmen können Sie für Blockierungsregeln und für Zulassungsregeln erstellen.

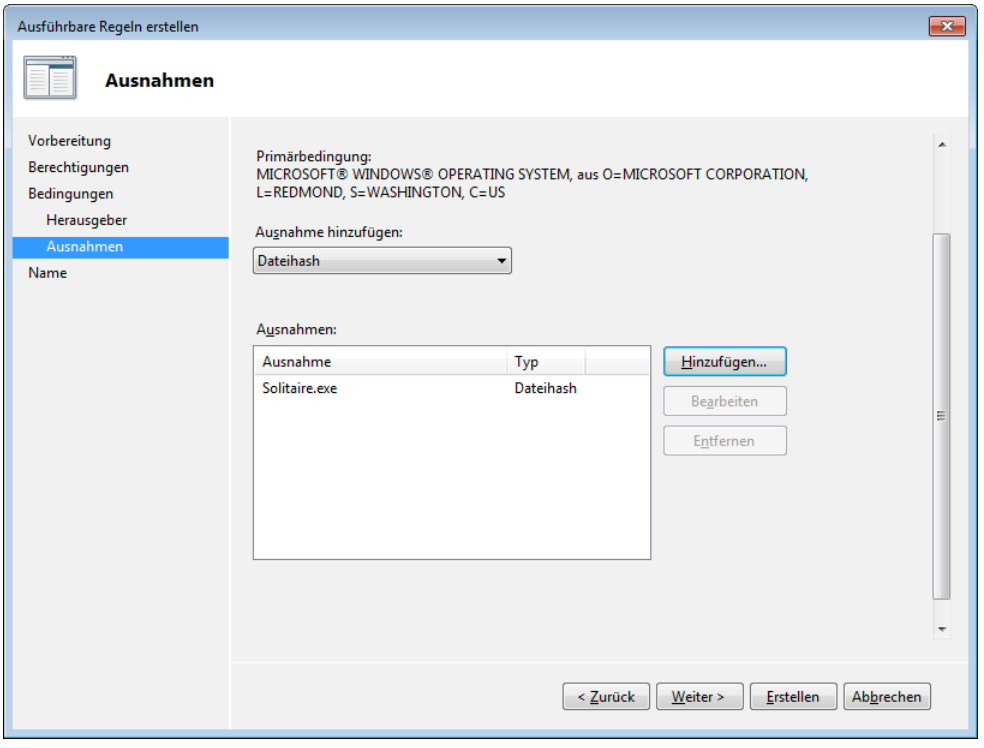


Abbildung 5.24 Konfigurieren einer Ausnahme

AppLocker-Überwachung

Da sich AppLocker in der Umgebung Ihrer Organisation sehr stark auf die Funktion der Anwendungen auswirken kann, ist es sinnvoll, die Funktionsweise von AppLocker zu überwachen, bevor die AppLocker-Richtlinien erzwungen werden. Auf diese Weise können Sie überprüfen, welche Anwendungen von AppLocker-Richtlinien betroffen sind, ohne die Ausführung dieser Anwendung tatsächlich zu blockieren. Wenn AppLocker die Regeln nur überwachen, aber nicht durchsetzen soll, konfigurieren Sie die betreffenden Regeltypen im Eigenschaftendialogfeld des Knotens *AppLocker* entsprechend (Abbildung 5.25).

AppLocker-Überwachungsereignisse werden im AppLocker-Ereignisprotokoll protokolliert, das in der Ereignisanzeige unter dem Knoten *Anwendungs- und Dienstprotokolle\Microsoft\Windows* angezeigt wird. Jeder Eintrag im AppLocker-Protokoll enthält folgende Informationen:

- Name der Regel
- SID des betroffenen Benutzers oder der betroffenen Gruppe
- Von der Regel betroffene Datei und Dateipfad
- Ob die Datei zugelassen oder blockiert wurde
- Regeltyp (Herausgeber, Pfad oder Dateihash)

In Kapitel 8, »BranchCache und Ressourcenfreigabe«, erfahren Sie mehr über das Thema Überwachung.

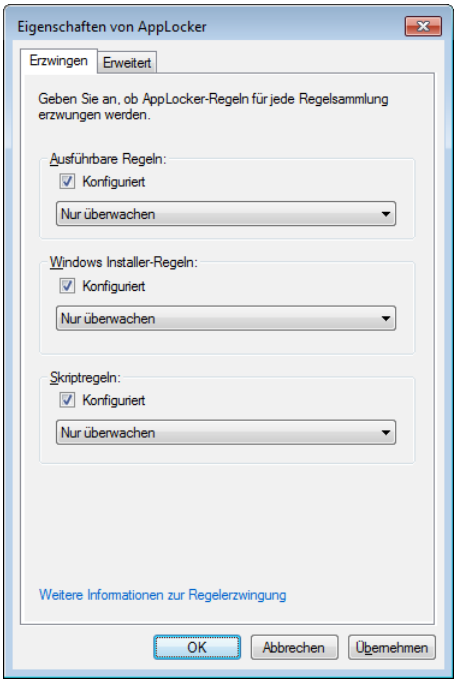


Abbildung 5.25 Konfigurieren der AppLocker-Überwachung



Weitere Informationen AppLocker-Überwachung

Weitere Informationen über die Konfiguration der AppLocker-Überwachung erhalten Sie in dem folgenden Microsoft TechNet-Artikel: *http://technet.microsoft.com/en-us/library/dd723693.aspx*.



Prüfungstipp

Stellen Sie sicher, dass Sie genau verstehen, warum ein Benutzer vielleicht in der Lage sein könnte, eine Anwendung auszuführen, ein anderer Benutzer aber nicht.

Übung Beschränken von Anwendungen

In dieser Übung verwenden Sie zwei verschiedene Methoden, um die Ausführung von Anwendungen zu beschränken: die Richtlinien für Softwareeinschränkung und AppLocker. Die Richtlinien für Softwareeinschränkung werden zur Beschränkung der Ausführung von Anwendungen unter Windows XP, Windows Vista und Windows 7 verwendet. AppLocker wurde mit Windows 7 eingeführt und ist nur in den Editionen Ultimate und Enterprise des Produkts verfügbar.

Übung 1 Konfigurieren einer Richtlinie für Softwareeinschränkung

In dieser Übung erstellen Sie eine Hashregel für eine Richtlinie für Softwareeinschränkung, um die Ausführung des Windows-Programms Rechner zu blockieren.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Klicken Sie auf *Start*, geben Sie **Rechner** ein und drücken Sie dann die EINGABE-TASTE. Überprüfen Sie, ob sich das Fenster der Anwendung Rechner öffnet, und schließen Sie dann die Anwendung.
3. Klicken Sie auf *Start*, geben Sie **gpedit.msc** ein und drücken Sie die EINGABE-TASTE. Dadurch öffnet sich die Konsole *Editor für lokale Gruppenrichtlinien*.
4. Navigieren Sie zum Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen*.
5. Wählen Sie den Knoten *Richtlinien für Softwareeinschränkung* und klicken Sie ihn mit der rechten Maustaste an. Wählen Sie *Neue Richtlinien für Softwareeinschränkung erstellen*.
6. Klicken Sie den Knoten *Zusätzliche Regeln* mit der rechten Maustaste an und wählen Sie *Neue Hashregel*. Dadurch öffnet sich das Dialogfeld *Neue Hashregel*. Klicken Sie auf *Durchsuchen*. Wechseln Sie in den Ordner *\Windows\System32*.
7. Geben Sie im Textfeld *Dateiname* des Dialogfelds *Öffnen* den Dateinamen **Calc.exe** ein und klicken Sie auf *Öffnen*. Sorgen Sie dafür, dass die Sicherheitsstufe *Nicht erlaubt* eingestellt ist (Abbildung 5.26), und klicken Sie dann auf *OK*.
8. Schließen Sie den Editor für lokale Gruppenrichtlinien und starten Sie den Computer dann neu. Melden Sie sich wieder mit dem Benutzerkonto *Kim_Akers* an.

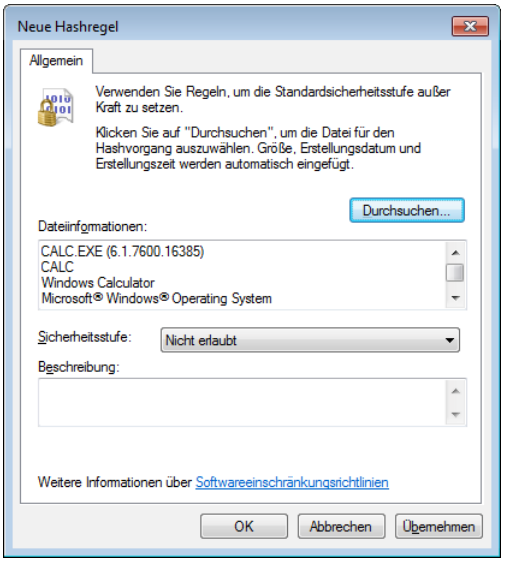


Abbildung 5.26 Erstellen einer Hashregel

9. Klicken Sie auf *Start*, geben Sie **Rechner** ein und drücken Sie dann die EINGABE-TASTE. Sie sollten die Meldung aus Abbildung 5.27 erhalten.

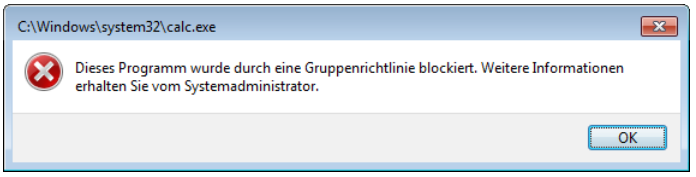

C:\Windows\system32\calc.exe
Dieses Programm wurde durch eine Gruppenrichtlinie blockiert. Weitere Informationen erhalten Sie vom Systemadministrator.
OK

Abbildung 5.27 Die Anwendung Rechner (*calc.exe*) wird durch eine Gruppenrichtlinie blockiert

10. Klicken Sie auf *Start*, geben Sie **gpedit.msc** ein und drücken Sie dann die EINGABE-TASTE. Dadurch öffnet sich die Konsole *Editor für lokale Gruppenrichtlinien*. Navigieren Sie zum Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für Softwareeinschränkung\Zusätzliche Regeln* und löschen Sie dann die Regel für *Calc.exe*.
11. Schließen Sie die Konsole *Editor für lokale Gruppenrichtlinien* und starten Sie den Computer dann neu. Melden Sie sich als *Kim_Akers* an und überprüfen Sie, ob Sie die Anwendung Rechner wieder öffnen können.

Übung 2 Konfigurieren von AppLocker

In dieser Übung richten Sie eine AppLocker-Richtlinie zum Blockieren der Anwendung Solitär ein.

1. Sofern Sie noch nicht auf dem Computer *Canberra* angemeldet sind, melden Sie sich als *Kim_Akers* an.
2. Klicken Sie auf *Start*, geben Sie **Solitär** ein und drücken Sie dann die EINGABE-TASTE. Überprüfen Sie, ob sich die Anwendung Solitär öffnet. Schließen Sie Solitär.

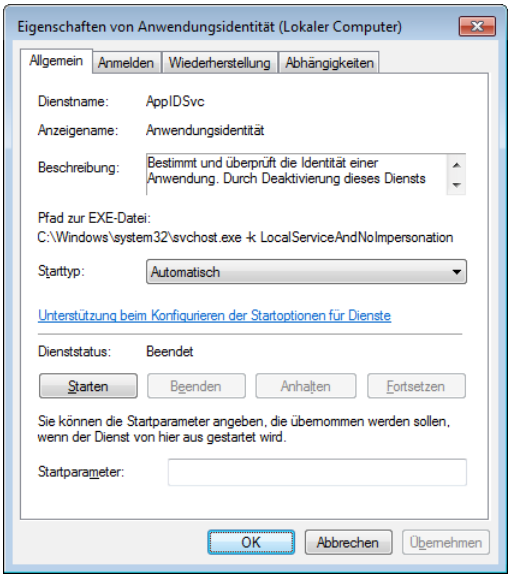


Abbildung 5.28 Konfigurieren des Starttyps des Dienstes *Anwendungsidentität*

3. Klicken Sie auf *Start*, geben Sie **services.msc** ein und drücken Sie dann die EINGABETASTE. Es öffnet sich die Konsole *Dienste*.
4. Klicken Sie den Dienst *Anwendungsidentität* mit einem Doppelklick an. Stellen Sie den Startup auf *Automatisch* (Abbildung 5.28). Klicken Sie auf *Starten* und dann auf *OK*. Schließen Sie die Konsole *Dienste*.
5. Klicken Sie auf *Start*, geben Sie **gpedit.msc** ein und drücken Sie die EINGABETASTE. Es öffnet sich die Konsole *Editor für lokale Gruppenrichtlinien*.
6. Navigieren Sie zum Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Anwendungssteuerungsrichtlinien* und wählen Sie das Element *AppLocker*.
7. Klicken Sie *Ausführbare Regeln* mit der rechten Maustaste an und wählen Sie *Neue Regel erstellen*. Klicken Sie auf der Seite *Vorbereitung* des Assistenten zum Erstellen von ausführbaren Regeln auf *Weiter*.
8. Wählen Sie auf der Seite *Berechtigungen* die Option *Verweigern* und klicken Sie auf *Weiter*.
9. Wählen Sie auf der Seite *Bedingungen* die Option *Herausgeber* und klicken Sie auf *Weiter*.
10. Klicken Sie auf der Seite *Herausgeber* auf *Durchsuchen*. Wechseln Sie in den Ordner *\Programme\Microsoft Games\Solitaire* und klicken Sie *Solitaire.exe* mit einem Doppelklick an.

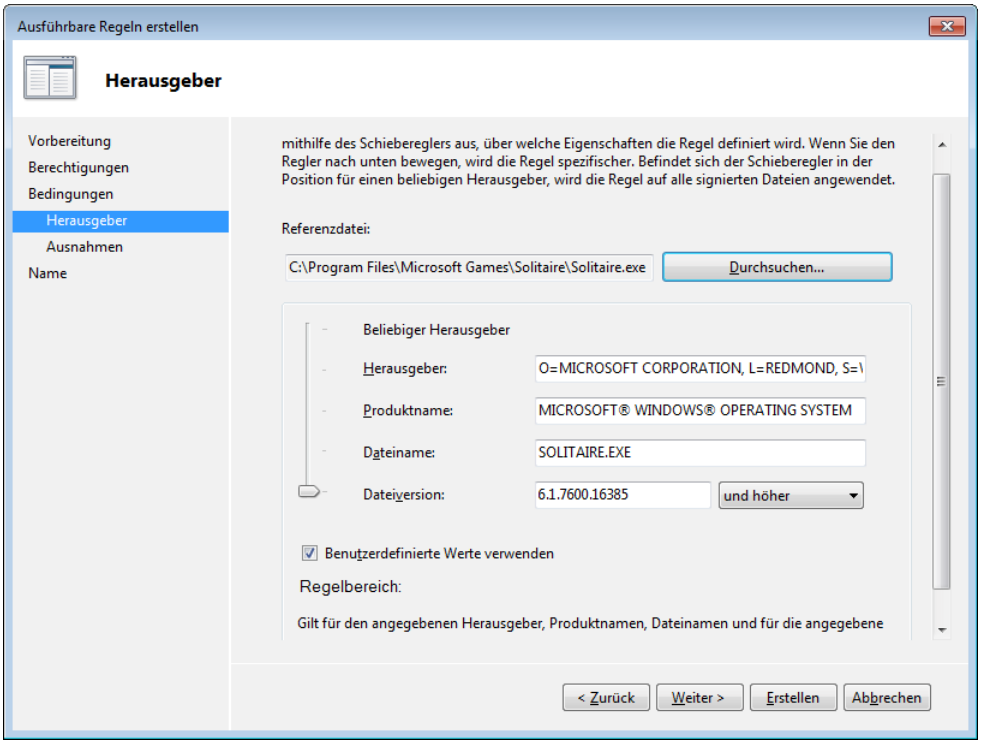


Abbildung 5.29 Eine Regel blockiert die Anwendung Solitär

11. Wählen Sie auf der Seite *Herausgeber* das Kontrollkästchen *Benutzerdefinierte Werte verwenden* und überprüfen Sie die Einstellungen anhand der Abbildung 5.29. Klicken Sie auf *Erstellen*.
12. Wenn Sie gefragt werden, ob Sie auch die Standardregeln erstellen möchten, klicken Sie auf *Ja*.
13. Schließen Sie die Konsole *Editor für lokale Gruppenrichtlinien* und starten Sie den Computer neu.
14. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* an und versuchen Sie, die Anwendung Solitär zu öffnen. Es sollte eine Meldung erscheinen, die Sie darüber informiert, dass die Anwendung von einer Richtlinie blockiert wird (Abbildung 5.30).

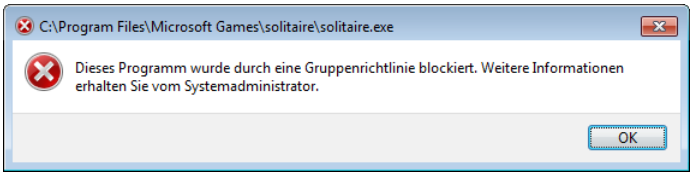

C:\Program Files\Microsoft Games\solitaire\solitaire.exe
Dieses Programm wurde durch eine Gruppenrichtlinie blockiert. Weitere Informationen erhalten Sie vom Systemadministrator.
OK

Abbildung 5.30 Solitär wird durch eine Gruppenrichtlinie blockiert

15. Klicken Sie auf *Start*, geben Sie **services.msc** ein und drücken Sie dann die EINGABETASTE. Es öffnet sich die Konsole *Dienste*.
16. Klicken Sie den Dienst *Anwendungsidentität* mit einem Doppelklick an. Stellen Sie den Starttyp *Deaktiviert* ein. Schließen Sie die Konsole *Dienste*.

Zusammenfassung der Lektion

- Richtlinien für Softwareeinschränkung können auf Computern verwendet werden, auf denen Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008 oder Windows 7 ausgeführt wird.
- Sie können in den Richtlinien für Softwareeinschränkung eine Standardregel wählen, die alle nicht zugelassenen Anwendungen blockiert, oder eine Standardregel, die alle Anwendungen zulässt, die nicht durch andere Regeln blockiert werden.
- Die spezielleren oder genauer formulierten Regeln der Richtlinien für Softwareeinschränkung haben Vorrang vor den allgemeiner formulierten Regeln. Eine Hashregel, die eine Anwendung zulässt, hat Vorrang vor einer Pfadregel, die dieselbe Anwendung sperrt.
- Hashregeln identifizieren Dateien anhand ihrer digitalen Fingerabdrücke. Wenn Sie eine Datei aktualisieren, müssen Sie dafür eine neue Hashregel erstellen.
- AppLocker-Richtlinien dienen zur Kontrolle von Anwendungen.
- AppLocker-Richtlinien können nur auf Computern verwendet werden, auf denen die Windows 7-Editionen Enterprise oder Ultimate ausgeführt werden.
- Die Pfad- und Hashregeln von AppLocker funktionieren wie die Pfad- und Hashregeln der Richtlinien für Softwareeinschränkung.

- Mit den AppLocker-Herausgeberregeln können Sie Regeln erstellen, mit denen überprüft wird, welcher Herausgeber eine Anwendung digital signiert hat. Mit Herausgeberregeln können Sie alle Anwendungen dieses Herausgebers, alle Versionen einer bestimmten Anwendung oder nur eine bestimmte Version der betreffenden Anwendung zulassen.
- Einige AppLocker-Regeltypen lassen Ausnahmen zu. Mit Ausnahmen können Sie eine bestimmte Anwendung von der Wirkung einer allgemeiner formulierten AppLocker-Regel ausnehmen.
- Eine AppLocker-Blockierungsregel hat immer Vorrang vor einer AppLocker-Zulassungsregel. Die Blockierungsgrundregel für AppLocker verhindert die Ausführung jeder Anwendung, die nicht ausdrücklich durch eine andere Regel zugelassen wird.
- AppLocker hat Vorrang vor den Richtlinien für Softwareeinschränkung, falls beide auf demselben Computer angewendet werden.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum aus Lektion 2, »Verwalten von AppLocker und der Richtlinien für Softwareeinschränkung«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Ihre Organisation verfügt über 50 Computer, auf denen Windows Vista zum Einsatz kommt, und über 40 Computer, auf denen Windows 7 Professional verwendet wird. Sie möchten verhindern, dass Benutzer das Spiel Solitär spielen können. Wie erreichen Sie dieses Ziel?
   A. Sie erstellen eine AppLocker-Herausgeberregel, die *Solitaire.exe* blockiert.
   B. Sie erstellen eine AppLocker-Hashregel, die *Solitaire.exe* blockiert.
   C. Sie erstellen eine AppLocker-Pfadregel, die *Solitaire.exe* blockiert.
   D. Sie erstellen eine Pfadregel für die Richtlinien für Softwareeinschränkung, die *Solitaire.exe* blockiert.
2. Welche Art von AppLocker-Regel erstellen Sie, um alle Anwendungen von einem bestimmten Hersteller zu sperren?
   A. Herausgeberregeln
   B. Pfadregeln
   C. Hashregeln
3. Sie möchten einige AppLocker-Regeln konfigurieren, mit denen die Ausführung aller nicht digital signierten Anwendungen eines Softwareherstellers verhindert wird. Sie möchten diese Regeln testen, bevor sie wirksam werden. Wie erreichen Sie dieses Ziel? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)

A. Sie erstellen AppLocker-Herausgeberregeln.
B. Sie erstellen AppLocker-Hashregeln.
C. Sie konfigurieren die AppLocker-Überwachung der ausführbaren Regeln.
D. Sie konfigurieren die AppLocker-Überwachung der Windows Installer-Regeln.

4. Ihre Organisation setzt unterschiedliche Computer ein, auf denen Windows 7 Ultimate oder Windows 7 Professional verwendet wird. Jede Computergruppe gehört zu einer separaten Organisationseinheit Ihrer Active Directory-Domänendiensteumgebung, auf deren Domänencontrollern Windows Server 2008 R2 verwendet wird. Sie haben für die Organisationseinheit, in der die Konten der Windows 7 Ultimate-Computer liegen, AppLocker-Richtlinien konfiguriert, um die Ausführung bestimmter Anwendungen zu verhindern. Für die Organisationseinheit, in der die Konten der Windows 7 Professional-Computer liegen, haben Sie Richtlinien für Softwareeinschränkung konfiguriert. Die Richtlinien für Softwareeinschränkung verhindern die Ausführung einiger Anwendungen, die für die Arbeit erforderlich sind. Die Anwendungen, die unter den Wirkungsbereich der AppLocker-Richtlinien fallen, funktionieren normal. Die erforderlichen Anwendungen werden also nicht blockiert. Wie können Sie sicherstellen, dass die AppLocker-Richtlinien richtig funktionieren?
   A. Sie konfigurieren die Gruppenrichtlinien so, dass der Dienst *Anwendungsverwaltung* automatisch gestartet wird. Sie wenden diese Richtlinie auf die Organisationseinheit an, in der die Konten der Windows 7 Ultimate-Computer liegen.
   B. Sie konfigurieren die Gruppenrichtlinien so, dass der Dienst *Anwendungsverwaltung* automatisch gestartet wird. Sie wenden diese Richtlinie auf die Organisationseinheit an, in der die Konten der Windows 7 Professional-Computer liegen.
   C. Sie konfigurieren die Gruppenrichtlinien so, dass der Dienst *Anwendungsidentität* automatisch gestartet wird. Sie wenden diese Richtlinie auf die Organisationseinheit an, in der die Konten der Windows 7 Ultimate-Computer liegen.
   D. Sie konfigurieren die Gruppenrichtlinien so, dass der Dienst *Anwendungsidentität* automatisch gestartet wird. Sie wenden diese Richtlinie auf die Organisationseinheit an, in der die Konten der Windows 7 Professional-Computer liegen.
5. Sie haben AppLocker-Richtlinien konfiguriert, die nur die Ausführung von bestimmten Anwendungen zulassen. Wenn für eine Anwendung keine AppLocker-Richtlinie vorhanden ist, kann sie nicht ausgeführt werden. Nach einer kürzlich erfolgten Softwareaktualisierung können Benutzer eine der Anwendungen, für die Sie eine Regel erstellt haben, nicht mehr verwenden. Die anderen Anwendungen funktionieren normal. Die fragliche Anwendung wurde vom Hersteller nicht digital signiert. Wie stellen Sie sicher, dass sich die Anwendung auf den Windows 7-Computern ausführen lässt?
   A. Sie erstellen für die Anwendung eine neue Hashregel.
   B. Sie erstellen für die Anwendung eine neue Herausgeberregel.
   C. Sie sorgen dafür, dass der Dienst *Anwendungsidentität* auf den Windows 7-Computern ausgeführt wird.
   D. Sie sorgen dafür, dass der Dienst *Anwendungsverwaltung* auf den Windows 7-Computern ausgeführt wird.

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Sie können die vordefinierten Kompatibilitätsmodi dazu benutzen, um Anwendungen, die für ältere Windows-Versionen entwickelt wurden, unter Windows 7 verwendbar zu machen. Wenn keiner der vordefinierten Kompatibilitätsmodi das Kompatibilitätsproblem löst, können Sie mit ACT eine große Datenbank mit anwendungsspezifischen Kompatibilitätsfixes und Kompatibilitätsmodi durchsuchen.
- Windows XP Mode ist eine virtuelle Version von Windows XP, die auf einem Clientcomputer unter Windows 7 Professional, Ultimate oder Enterprise verwendet werden kann, um Kompatibilitätsprobleme zu lösen, die sich mit den vordefinierten Kompatibilitätsmodi oder mit ACT nicht lösen lassen.
- Die Richtlinien für Softwareeinschränkung können auf allen Windows-Versionen verwendet werden und ermöglichen die Erstellung von Regeln auf der Basis von Dateihashwerten, Softwarepfaden, Herausgeberzertifikaten oder Netzwerkzonen. Die Richtlinien für Softwareeinschränkung werden von der speziellsten bis hin zur allgemeinsten Richtlinie angewendet. Speziellere oder genauer formulierte Regeln haben Vorrang vor allgemeineren Regeln.
- AppLocker-Richtlinien können nur auf Computern verwendet werden, auf denen die Editionen Windows 7 Enterprise oder Ultimate ausgeführt werden. AppLocker-Richtlinien lassen sich auf der Basis der Herausgeberidentität, eines Dateihashwerts oder eines Softwarepfads definieren. AppLocker bietet Assistenten, die die Regeln automatisch erstellen. AppLocker-Blockierungsregeln haben Vorrang vor allen anderen AppLocker-Regeln.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **AppLocker-Richtlinie**
- **Kompatibilitätsfix**
- **Kompatibilitätsmodus**
- **Hashregel**
- **Pfadregel**
- **Herausgeberregel**
- **Richtlinie für Softwareeinschränkung**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie Ihr Wissen zu den Themen dieses Kapitels an. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: Konfigurieren der Anwendungskompatibilität bei Fabrikam

Sie planen die Umstellung der Desktopcomputer Ihrer Organisation von Windows XP auf Windows 7. Zurzeit untersuchen Sie Anwendungskompatibilitätsprobleme und sind hauptsächlich mit den drei Anwendungen Alpha, Beta und Gamma beschäftigt. Bei der Überprüfung finden Sie heraus, dass Alpha zwar problemlos auf Computern läuft, auf denen Windows XP Professional SP3 installiert ist, aber nicht auf Windows 7 Enterprise. Anwendung Beta läuft unter Windows 7, wenn Sie die Verknüpfung mit der Anwendung auf dem Desktop mit der rechten Maustaste anklicken und dann auf *Als Administrator ausführen* klicken. Die Anwendung Gamma wurde erstellt, als es in der Organisation eine kleine Entwicklergruppe gab. Mit den vordefinierten Windows 7-Kompatibilitätsmodi funktioniert die Anwendung nicht. Ihre Organisation verfügt nicht mehr über die Fachkenntnis, den ursprünglichen Quellcode zu verstehen und so zu ändern, dass die Anwendung unter Windows 7 läuft. Beantworten Sie nun folgende Fragen:

Fragen

1. Was müssen Sie tun, damit sich die Anwendung Alpha ausführen lässt?
2. Was können Sie tun, damit sich die Anwendung Beta durch einen simplen Klick auf ihre Verknüpfung starten lässt?
3. Mit welchem Tool können Sie für die Anwendung Gamma benutzerdefinierte Kompatibilitätsoptionen konfigurieren?

Übung 2: Beschränken von Anwendungen bei Contoso

Sie sind in der Antarktis-Forschungsstation von Contoso für die Konfiguration von Computern zuständig, auf denen Windows 7 Enterprise verwendet wird. Die Entwicklungsabteilung von Contoso hat eine Anwendung zur Datenerfassung und Datenanalyse entwickelt, die in der Forschungsstation verwendet wird. Diese Anwendung kommuniziert mit Instrumenten,

die in der Umgebung des Contoso-Außenpostens Temperaturschwankungen in den Eisfeldern messen. Die Entwickler haben die Anwendung nicht digital signiert. Da die Anwendung mit empfindlichen wissenschaftlichen Instrumenten kommuniziert, dürfen nur Mitglieder der Gruppe *Scientists* die Datenerfassungsanwendung verwenden. Sie möchten die Ausführung der Anwendung nun mit einer passenden Regel einschränken. Beantworten Sie vor diesem Hintergrund nun folgende Fragen.

Fragen

1. Welche Art von Regel würden Sie für die Datenerfassungsanwendung erstellen?
2. Wie können Sie sicherstellen, dass nur Mitglieder der Gruppe *Scientists* und keine anderen Benutzer die Datenerfassungsanwendung verwenden können?
3. Was müssten die Entwickler der Anwendung tun, damit Sie eine Herausgeberregel für die Anwendung erstellen können?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Konfigurieren der Anwendungskompatibilität

In diesen Übungen konfigurieren Sie die Anwendungskompatibilität. Verwenden Sie Ihre Lieblingssuchmaschine, um eine Testversion einer Anwendung zu suchen und herunterzuladen, die unter einer älteren Windows-Version funktioniert, aber nicht unter Windows 7.

- **Übung 1** Bearbeiten Sie die Eigenschaften einer Anwendung und konfigurieren Sie einen Windows 7-Kompatibilitätsmodus, mit dem die Anwendung auch unter Windows 7 verwendbar ist.
- **Übung 2** Bearbeiten Sie die Eigenschaften einer Anwendung und konfigurieren Sie einen Windows 7-Kompatibilitätsmodus so, dass die Benutzeroberfläche Aero bei der Ausführung der Anwendung deaktiviert wird.

Konfigurieren von Anwendungseinschränkungen

In diesen Übungen konfigurieren Sie Anwendungseinschränkungen. Für die Übungen müssen Sie die Anwendung Process Explorer auf den Desktop Ihres Windows 7-Computers herunterladen. Sie finden die Anwendung unter *http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx*. Außerdem müssen Sie zur Durchführung dieser Übung den Dienst *Anwendungsidentität* temporär aktivieren. Vergessen Sie nicht, diesen Dienst nach den Übungen wieder zu deaktivieren, damit es in den folgenden Kapiteln nicht zu Problemen mit der Ausführung von anderen Anwendungen kommt.

- **Übung 1** Konfigurieren Sie im Editor für lokale Gruppenrichtlinien eine AppLocker-Pfadregel, mit der Sie die Ausführung der Anwendung Process Explorer verhindern, die Sie in den Übungen von Lektion 1 heruntergeladen haben. Überprüfen Sie nach dem Neustart des Computers, ob die Anwendung durch die Pfadregel blockiert wird. Erstellen Sie anschließend an einem anderen Ort eine Kopie der ausführbaren Datei. Versuchen Sie, die Anwendung an diesem neuen Speicherort auszuführen.

- **Übung 2** Erstellen Sie im Editor für lokale Gruppenrichtlinien eine Herausgeberregel, die die Ausführung der Anwendung Process Explorer verhindert. Überprüfen Sie nach dem Neustart des Computers, ob sich die Anwendung Process Explorer starten lässt. Kopieren Sie die Anwendungsdatei an einen anderen Ort. Überprüfen Sie, ob sich die Anwendung Process Explorer am neuen Speicherort ausführen lässt.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

K A P I T E L 6

Netzwerkeinstellungen

Dieses Kapitel befasst sich mit Netzwerken und erklärt, wie Sie Computer und andere Geräte in einem Netzwerk finden. Es stellt Internet Protocol Version 4 (IPv4) vor, ein robustes, zuverlässiges Protokoll, das seit vielen Jahren Routing implementiert und Pakete an Hosts in Subnetzen ausliefert. Außerdem beschreibt es die verschiedenen Arten der IPv4-Adressen und die Dienste, auf denen IPv4 aufbaut.

Internet Protocol Version 6 (IPv6) ist der Nachfolger von IPv4, und dieses Kapitel erklärt, warum IPv4 für moderne Netzwerke, insbesondere das Internet, wahrscheinlich nicht mehr ausreicht. Es beschreibt die verschiedenen Arten von IPv6-Adressen und ihre Aufgabe sowie die Adresstypen, mit denen der Übergang von IPv4 auf IPv6 implementiert wird.

Früher arbeiteten die meisten Netzwerke mit Kabelverbindungen, aber Drahtlosnetzwerke sind stark im Kommen, vor allem aufgrund des Anstiegs bei der mobilen Kommunikation und der Arbeit zu Hause. Das Kapitel erklärt, wie Sie sowohl Kabel- als auch Drahtlosnetzwerke einrichten und Verbindungsprobleme beseitigen.

Zuletzt befasst sich das Kapitel mit dem neuen Windows 7-Feature des standortabhängigen Druckens, das es mobilen Benutzern ermöglicht, zwischen Netzwerken zu wechseln, ohne ihren Standarddrucker umstellen zu müssen.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von IPv4-Netzwerkeinstellungen
- Konfigurieren von IPv6-Netzwerkeinstellungen
- Konfigurieren von Netzwerkeinstellungen

Lektionen in diesem Kapitel:

- Lektion 1: Konfigurieren von IPv4 297
- Lektion 2: Konfigurieren von IPv6 326
- Lektion 3: Netzwerkkonfiguration 345

Bevor Sie beginnen

Um die Übungen in diesem Kapitel durchzuarbeiten, müssen Sie folgende Vorbereitungen getroffen haben:

- Sie haben Windows 7 auf einem eigenständigen Client-PC installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben. Sie brauchen Internetzugriff, um die Übungen durchzuführen.
- Sie haben Windows 7 auf einem zweiten PC installiert. Dabei gehen Sie genauso vor wie beim Einrichten des ersten PCs. Benutzername und Kennwort sind gleich (*Kim_Akers* und *P@ssw0rd*). Der Computername ist *Aberdeen*. Übernehmen Sie wie bei der Installation des Computers *Canberra* die Standardeinstellungen (sofern Sie keine andere Tastatur benutzen oder in einer anderen Zeitzone arbeiten). Es wird dringend empfohlen, den Computer *Aberdeen* als virtuellen Computer anzulegen. Dafür können Sie Hyper-V verwenden oder Microsoft Virtual PC 2007 unter *http://www.microsoft.com/downloadS/details.aspx?FamilyID=04d26402-3199-48a3-afa2-2dc0b40a73b6* herunterladen.
- Falls Sie zwei physische Computer benutzen, die nicht im selben Netzwerk liegen, müssen Sie ihre Ethernetanschlüsse mit einem Crossoverkabel oder mithilfe eines Ethernetswitchs verbinden.
- Um die optionale Übung in Lektion 1 durchzuarbeiten, brauchen Sie eine Drahtlosverbindung auf dem Computer *Canberra* und einen Drahtloszugriffspunkt (Wireless Access Point, WAP), der über ein DSL-Modem mit dem Internet verbunden ist. Für die Übung in Lektion 3, »Netzwerkkonfiguration«, weiter unten in diesem Kapitel brauchen Sie auf beiden Computern jeweils einen Drahtlosadapter.

Praxistipp

Ian McLean

Ich habe gerade gelesen – und zwar in einer Microsoft-Zeitschrift, also muss es stimmen –, dass uns die IPv4-Adressen ausgehen.

Als jemand, der bereits 1999 eindringlich vor dieser Gefahr gewarnt hat, kann ich nicht behaupten, ich wäre überrascht. Mich überrascht lediglich, dass es so lange gedauert hat. Der Einsatz von NAT (Network Address Translation) und privaten Adressbereichen, von CIDR (Classless Inter-Domain Routing) und VLSM (Variable-Length Subnet Mask) und das verbissene Zurückholen zugewiesener, aber unbenutzter Adressen konnten das Unvermeidliche letztlich nur aufschieben. Sie waren niemals eine dauerhafte Lösung. Wir haben eine begrenzte Ressource verbraucht. Wir konnten diesen Prozess verlangsamen, aber nicht aufhalten. Wie sieht also eine echte Lösung aus?

Kurz gesagt (ganz kurz, schließlich ist es ein Akronym): IPv6.

Es wurde eine Unmenge Geld in das IPv4-Internet investiert, daher wird es nicht über Nacht verschwinden. Als Profi müssen Sie sich also mit IPv4 auskennen und wissen, wie Sie es konfigurieren und damit arbeiten. Daran wird sich etliche Jahre nichts ändern. Aber inzwischen gibt es Inseln des IPv6-Internets im Meer des IPv4-Internets. IPv6 wächst schnell und irgendwann wird IPv4 die Inseln bilden, die immer kleiner werden.

Sie dürfen also nicht IPv4 ignorieren, aber es ist an der Zeit, IPv6 in den Katalog Ihrer Fachkenntnisse aufzunehmen. Schließlich ist es alles andere als neu. Das IPv6-Internet gibt es schon seit dem letzten Jahrtausend. Sie brauchen keine Subnetze oder Supernetze dafür, und ein Gerät kann mehrere IPv6-Adressen für unterschiedliche Funktionen haben. Es gibt darin eine wirklich unglaubliche Zahl verfügbarer Adressen. Angeblich ist die Ressource praktisch unerschöpflich. (Hm, wurde so etwas nicht auch 1985 über den IPv4-Adressraum behauptet?)

Arbeiten Sie sich also in IPv6 ein. An Ihrer Stelle würde ich mich damit beeilen. Die Menschheit ist immer dann am erfinderischsten, wenn sie sich daran macht, eine praktisch unerschöpfliche Ressource aufzubrauchen. Wahrscheinlich bin ich etwas voreilig, aber ich habe bereits Wetten mit einigen Kollegen laufen, dass IPv8 eingeführt wird, bevor ich zur letzten Ruhe gebettet werde. (Was sie wohl nicht bedacht haben: Wie wollen sie einen eventuellen Gewinn geltend machen?)

Lektion 1: Konfigurieren von IPv4

Als IT-Experte mit mindestens ein Jahr Erfahrung hatten Sie garantiert schon mit IPv4-Adressen, Subnetzmasken und Standardgateways zu tun. Sie wissen, dass in Unternehmensumgebungen DHCP-Server die IPv4-Einstellungen automatisch konfigurieren und DNS-Server (Domain Name System) Computernamen in IPv4-Adressen auflösen.

Sie haben wahrscheinlich schon kleinere Testnetzwerke mit statischen IPv4-Adressen konfiguriert. Allerdings rufen inzwischen selbst die kleinsten Netzwerke ihre Konfiguration meist von einem DSL-Router oder WAP ab, der wiederum von einem Internetprovider (Internet Service Provider, ISP) konfiguriert wird. Unter Umständen haben Sie die gemeinsame Nutzung der Internetverbindung eingerichtet, bei der Clientcomputer über den Umweg über einen anderen Clientcomputer auf das Internet zugreifen und ihre Konfiguration abrufen.

Wahrscheinlich hatten Sie beim Debuggen von Verbindungsproblemen schon mit APIPA-Adressen (Automatic Private Internet Protocol Addressing) zu tun, die mit 168.254 beginnen. Falls Computer ihre IPv4-Adresskonfiguration nicht von DHCP erhalten, weisen sie sich selbst normalerweise APIPA-Adressen zu. Eine APIPA-Adresse deutet daher oft auf einen DHCP-Ausfall oder den Verlust der Konnektivität hin. Prinzipiell ist es allerdings eine einwandfreie Methode, um isolierte Netzwerke zu konfigurieren, die nicht mit anderen Netzwerken wie dem Internet kommunizieren.

Weniger wahrscheinlich ist, dass Sie am Netzwerkentwurf mitgearbeitet oder ein Netzwerk in Subnetze unterteilt haben. Die Subnetzunterteilung wird heutzutage nicht mehr so oft eingesetzt, weil private Netzwerke und NAT Ihnen sehr viele Adressen zur Verfügung stellen, die Sie verwenden können. In den guten alten Zeiten, als alle Adressen öffentlich waren und die Administratoren ihre zugewiesenen Adressbereiche optimal nutzen mussten, war die Subnetzunterteilung eine wichtige Fähigkeit. Trotzdem bleibt die Subnetzunterteilung nach wie vor nützlich, und das Thema Subnetzmasken taucht wahrscheinlich in der Prüfung 70-680 auf.

In dieser Lektion sehen Sie sich die Tools an, die zum Bearbeiten von IPv4-Adressen und Subnetzmasken sowie zum Einrichten von IPv4-Netzwerkverbindungen zur Verfügung stehen. Die Lektion stellt das Netzwerk- und Freigabecenter vor, die Befehlszeilentools Netstat und Netsh und die Windows-Netzwerkdiagnose. Sie erklärt, wie Sie einen Computer

mit einem Netzwerk verbinden, wie Sie die Namensauflösung konfigurieren, wie APIPA funktioniert, wie Sie einen Verbindung für ein Netzwerk einrichten, wie Sie Netzwerkstandorte einrichten und wie Sie Konnektivitätsprobleme beseitigen.

Bevor Sie sich alle Tools zum Bearbeiten und Konfigurieren von IPv4 ansehen, müssen Sie wissen, wie Adressen und Subnetzmasken aufgebaut sind. Sie erfahren, welche Bedeutung Adressen wie 10.0.0.21, 207.46.197.32 und 169.254.22.10 haben. Sie lernen, warum 255.255.255.128, 255.255.225.0, 225.255.254.0 und 255.255.252.0 gültige Subnetzmasken sind, 255.255.253.0 aber nicht. Und Sie erfahren, welche Auswirkung es auf die mögliche Größe Ihres Netzwerks hat, wenn Sie die Subnetzmaske ändern, und warum APIPA-Adressen keine Standardgateways haben.

Dieses Kapitel beginnt mit einer Einführung in IPv4, insbesondere IPv4-Adressen, Subnetzmasken und Standardgateways. Dann konzentriert es sich auf die praktischen Aspekte beim Konfigurieren und Verwalten eines Netzwerks.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Erklären der Funktionen einer IPv4-Adresse, einer Subnetzmaske und eines Standardgateways und Verstehen des Punkt-Dezimal-Formats
- Verbinden von Arbeitsstationen mit einem Kabelnetzwerk und Einrichten von ICS (Internet Connection Sharing) in diesem Netzwerk
- Verwalten von Verbindungen in Kabelnetzwerken

Veranschlagte Zeit für diese Lektion: 50 Minuten

Grundlagen von IPv4-Adressen

IPv4 steuert die Reihenfolge und Auslieferung von Paketen. Jedes ein- oder ausgehende Paket (auch als Datagramm bezeichnet) enthält die Quell-IPv4-Adresse des Absenders und die Ziel-IPv4-Adresse des Empfängers. IPv4 ist für das Routing verantwortlich. Werden Informationen an ein anderes Gerät innerhalb eines Subnetzes übertragen, wird das Datagramm an die entsprechende interne IPv4-Adresse gesendet. Falls das Datagramm dagegen an ein Ziel gesendet wird, das außerhalb des lokalen Subnetzes liegt (wenn Sie beispielsweise auf das Internet zugreifen), untersucht IPv4 die Zieladresse, vergleicht sie mit einer Routentabelle und entscheidet, welche Aktion durchgeführt werden soll.

Sie können sich die IPv4-Konfiguration auf einem Computer ansehen, indem Sie das Eingabeaufforderungsfenster öffnen. Dazu klicken Sie entweder im Menü *Alle Programme* auf *Zubehör* und dann auf *Eingabeaufforderung* oder geben im Suchfeld des Startmenüs den Befehl **cmd** ein. Wenn Sie die Konfiguration ändern wollen, statt sie nur anzuzeigen, müssen Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen.

Das Befehlszeilentool Ipconfig zeigt die IPv4-Einstellungen (und IPv6-Einstellungen) eines Computers an. Abbildung 6.1 zeigt die Ausgabe von Ipconfig auf einem Computer, der über einen WAP drahtlos mit dem Internet verbunden ist und intern an ein privates Kabelnetzwerk angeschlossen ist, das über APIPA konfiguriert wird. Ausführlichere Informationen liefert der Befehl **ipconfig /all**.

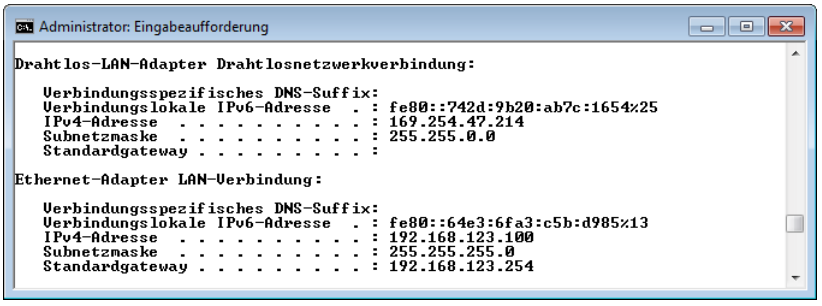

Administrator: Eingabeaufforderung
Drahtlos-LAN-Adapter Drahtlosnetzwerkverbindung:
Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse . : fe80::742d:9b20:ab7c:1654%25
IPv4-Adresse . . . . . : 169.254.47.214
Subnetzmaske . . . . . : 255.255.0.0
Standardgateway . . . . . :
Ethernet-Adapter LAN-Verbindung:
Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse . : fe80::64e3:6fa3:c5b:d985%13
IPv4-Adresse . . . . . : 192.168.123.100
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 192.168.123.254

Abbildung 6.1 Ausgabe des Befehls `ipconfig`

Die IPv4-Adresse identifiziert den Computer und das Subnetz, in dem sich der Computer befindet. Eine IPv4-Adresse muss innerhalb eines Netzwerks eindeutig sein. Hier ist die private Adresse eindeutig innerhalb des internen Netzwerks (die Zahl 10 am Anfang der Adresse verrät, dass es sich um eine private Adresse handelt). Ist die IPv4-Adresse eine öffentliche Adresse im Internet, muss sie im gesamten Internet einmalig sein. Öffentliche und private Adressen sehen wir uns weiter unten in dieser Lektion noch genauer an.

An der IPv4-Adresse ist nichts Geheimnisvolles. Es ist einfach eine Zahl aus einem sehr großen Wertebereich. Sie wird in einem Format geschrieben, das als Punkt-Dezimal-Notation (dotted decimal notation) bezeichnet wird. Dieses Format lässt sich von uns Menschen bequem verarbeiten. Eine IPv4-Adresse ist eine Zahl mit 32 binären Ziffern (Bits), wobei jedes Bit den Wert 1 oder 0 haben kann. Sehen Sie sich als Beispiel die folgende Binärzahl an:

00001010 00010000 00001010 10001111

Die Leerzeichen sind ohne Bedeutung, sie haben lediglich die Aufgabe, die Zahl besser lesbar zu machen.

Der dezimale Wert dieser Zahl ist 168.823.439. In hexadezimaler Schreibweise ist das 0A100A8F. Keine dieser Methoden, die Zahl auszudrücken, ist intuitiv oder bequem.



Hinweis Binäre und hexadezimale Notation

Sie brauchen kein Mathematiker oder Experte in binärer Notation zu sein, um IPv4-Adressen zu verstehen. Einige Grundkenntnisse sind aber unverzichtbar. Sie können sich genauer informieren, indem Sie (beispielsweise) im Internet nach »Binärsystem« suchen, aber eine der besten Methoden, sich mit binären und hexadezimalen Zahlen vertraut zu machen, besteht darin, den wissenschaftlichen Rechner zu starten, der in Windows 7 enthalten ist. Schalten Sie dazu auf Binärnotation um (*Bin*) und geben Sie **11111111** ein. Schalten Sie dann auf Dezimal- (*Dez*) und Hexadezimalnotation (*Hex*) um. Sie erhalten daraufhin die Zahlen 255 beziehungsweise FF. Derselbe Rechner steht Ihnen auch in der Prüfung 70-680 zur Verfügung.

Binärzahlen werden aber im Allgemeinen in Gruppen mit 8 Ziffern unterteilt, die sogenannten Oktette (ein Informatiker würde sie Bytes nennen). Unterteilen wir die Beispielzahl also in vier Oktette und setzen wir jeweils einen Punkt zwischen zwei Gruppen, weil Punkte einfacher zu sehen sind als Leerzeichen:

00001010.00010000.00001010.10001111

Konvertieren Sie die binäre Zahl in jedem Oktett in eine Dezimalzahl. Sie erhalten:

10.16.10.143

Binär, Dezimal, Hexadezimal und Punkt-Dezimal sind unterschiedliche Methoden, dieselbe Zahl auszudrücken. Die Zahl identifiziert den Computer (oder eine andere Netzwerkkomponente) eindeutig innerhalb eines Netzwerks und gibt an, in welchem eindeutigen Netzwerk (oder Subnetz) er sich befindet.

Ein Netzwerk wird in ein oder mehrere Subnetze unterteilt. Kleine Netzwerke, etwa Testnetzwerke, bestehen oft nur aus einem einzigen Subnetz. Unterschiedliche Subnetze sind über einen Router miteinander verbunden. Dieser Router kann beispielsweise ein WAP (Wireless Access Point), ein Microsoft-Server, der als Router konfiguriert ist, oder ein Hardwaregerät wie ein Cisco- oder 3Com-Router sein. Jedes Subnetz hat seine eigene Subnetzadresse innerhalb des Netzwerks und seine eigene Gateway- oder Routerverbindung. In großen Netzwerken können manche Subnetze mit mehreren Routern verbunden sein. Sie können auch die Verbindung über ein Modem zu einem Internetprovider als Subnetz betrachten, das wiederum über einen Router beim Internetprovider mit dem Internet verbunden ist.

Welcher Teil der Adresse identifiziert nun den Computer und welcher das Subnetz? Um das herauszufinden, müssen wir uns den nächsten Wert in der Ausgabe von Ipconfig ansehen, die Subnetzmaske. Subnetzmasken (subnet mask) sind recht seltsame Zahlen. Sie sind binäre Zahlen, die aus einer ununterbrochenen Folge von Einsen, gefolgt von einer ununterbrochenen Folge von Nullen, bestehen. Zum Beispiel ist

255.255.255.0

die binäre Zahl

11111111 11111111 11111111 00000000

Der tatsächliche Wert dieser Zahl ist unerheblich, worauf es ankommt, ist die Zahl der Einsen und Nullen. Eine Eins besagt, dass das entsprechende Bit in der IPv4-Adresse ein Bit der Netzwerkadresse ist. Eine Null besagt, dass das entsprechende Bit in der IPv4-Adresse ein Bit der Computer- oder Hostadresse ist.

In unserem Beispiel sind die hinteren 8 Bits der Subnetzmaske Nullen. Die Hostadresse ist also das letzte Oktett der IPv4-Adresse, 143. Die Netzwerkadresse des Subnetzes ist 10.16.10.0. Weil Hosts in diesem Beispiel durch ein einziges Oktett definiert werden, enthält das Subnetz 10.16.10.0 insgesamt 254 Hostadressen. Die erste IPv4-Adresse in diesem Subnetz lautet 10.16.10.1, die letzte 10.16.10.254. Die Zahl 10.16.10.0 identifiziert das Subnetz selbst, sie wird als Subnetzadresse bezeichnet. Die Zahl 10.16.10.255 ist die sogenannte Broadcastadresse. Sie wird verwendet, wenn ein Paket an alle Hosts in einem Subnetz gesendet werden soll.

Subnetze und Supernetze

Sie können ein Subnetz in kleinere Subnetze unterteilen, indem Sie zu den Einsen der Subnetzmaske weitere Einsen hinzufügen. Falls Sie zwei (oder mehrere) Subnetze aus zusammenhängenden Zahlenbereichen haben, können Sie sie zu einem einzigen Subnetz zusammenfassen, indem Sie eine oder mehrere Einsen am Ende der Einsenfolge in den Subnetzmasken zu Nullen machen. Diese Techniken werden als *Subnetzunterteilung* (subnetting) beziehungsweise *Supernetze* (supernetting) bezeichnet.

Wenn eine Organisation viele Computer in ihrem Netzwerk hat (mehr als 100, die Zahl hängt von Typ, Volumen und Verkehrsmuster im Netzwerk ab) oder Filialen an unterschiedlichen Orten, erstellt sie wahrscheinlich mehrere Subnetze. Enthält ein Subnetz zu viele Computer und andere Geräte, wird es oft langsamer, weil die Wahrscheinlichkeit größer wird, dass zwei Computer gleichzeitig versuchen, Daten ins Netzwerk zu senden, sodass eine Kollision entsteht. Wird ein Netzwerk in mehrere Subnetze unterteilt, sinkt die Wahrscheinlichkeit, dass solche Kollisionen auftreten.

Beim Router, der die Verbindung zum Internet herstellt, implementiert die Organisation dagegen ein Supernetz, um die Subnetze zu kombinieren (zusammenzufassen), sodass sie mit einer einzigen Netzwerkadresse definiert werden können, die in eine öffentliche Adresse im Internet umgesetzt wird. Öffentliche Adressen und Adressumsetzung werden weiter unten in dieser Lektion beschrieben.



Weitere Informationen Subnetze und Supernetze

Weitere Informationen über Supernetze und Subnetzunterteilung sowie über CIDR und VLSM finden Sie unter *http://support.microsoft.com/kb/164015*.



Hinweis CIDR-Notation

Die Subnetzmaske 255.255.255.0 besteht aus 24 Einsen gefolgt von 8 Nullen, Sie können sie daher auch als »/24« schreiben. Zum Beispiel wird ein Subnetz mit der Netzwerkadresse 192.168.0.0 und der Subnetzmaske 255.255.255.0 dann als 192.168.0.0/24 angegeben. Dies wird manchmal als *CIDR-Notation* bezeichnet. Eine Subnetzmaske mit 25 Einsen, gefolgt von 7 Nullen, wird als Subnetzmaske /25 geschrieben. In Punkt-Dezimal-Notation wäre das 255.255.255.128.

Der letzte Wert in Abbildung 6.1 ist das *Standardgateway*. Dies ist die IPv4-Adresse der Routerverbindung im selben Subnetz wie die IPv4-Adresse des Hostcomputers. Falls die Zieladresse eines IPv4-Pakets in einem anderen Subnetz liegt, wird das Paket über den Router durch andere Subnetze weitergeleitet, bis es am gesuchten Ziel angelangt ist. Wenn Sie zum Beispiel im Browser eine Website aufrufen, müssen Sie Daten an den Webserver der Site schicken, dessen IPv4-Adresse irgendwo im Internet liegt.

Einfach ausgedrückt: Manche Pakete müssen Ihr Subnetz verlassen und in ein anderes Netzwerk gelangen (zum Beispiel das Internet). Ihr Computer sendet diese Pakete an ein Routinggerät. Dies kann ein Hardwarerouter sein, ein Server, der als Router konfiguriert ist, oder der Computer oder Drahtlosrouter, über den die anderen Computer in einem SOHO-Netzwerk (Small Office/Home Office) auf das Internet zugreifen. Das Standardgateway ist die Adresse innerhalb des Subnetzes des Routinggeräts (das mindestens eine weitere IPv4-Adresse in einem anderen Subnetz hat). Über das Standardgateway verlassen die ausgehenden Pakete das Subnetz. An dieser Stelle treten auch eingehende Pakete von anderen Netzwerken in das Subnetz ein.

Schnelltest

1. Wie lautet die binäre Zahl 00001010 11110000 10101010 01000000 in Punkt-Dezimal-Notation?
2. Liegen die IPv4-Adressen 192.168.1.200 und 192.168.1.24 im selben Subnetz? Beide haben die Subnetzmaske 255.255.255.0.
3. Ist 10.0.0.130 eine gültige IPv4-Adresse im Subnetz 10.0.0.0/25?

Antworten zum Schnelltest

1. 10.240.170.64.
2. Die Subnetzmaske verrät, dass das letzte Oktett die Hostadresse bildet. Daher bilden die vorderen drei Oktette die Netzwerkadresse des Subnetzes. In beiden Fällen ist dies 192.168.1.0, die Computer liegen also im selben Subnetz.
3. Nein. Die Subnetzmaske /25 enthält 25 Einsen und daher 32 – 25 = 7 Nullen. Nullen geben an, welcher Teil der Adresse die Hostadresse enthält. Daher reicht der Bereich der Hostadressen von 0000001 bis 1111110 binär (0000000 ist die Netzwerkadresse, und 111111 die Broadcastadresse). In Dezimalnotation entspricht dies 1 bis 126. Die gültigen IPv4-Adressen im Netzwerk sind also 10.0.0.1 bis 10.0.0.126. Die Adresse 10.0.0.130 befindet sich nicht in diesem Bereich, daher ist sie in diesem Subnetz nicht gültig. Es ist eine Adresse in einem anderen Subnetz (beispielsweise in 10.0.0.128/25).

Netzwerkdienste

Konfiguration und Betrieb von IPv4 hängen von mehreren Netzwerkdiensten ab. In einer Unternehmensumgebung werden diese Dienste (außer APIPA) auf Servern implementiert. Dagegen können DHCP- und DNS-Dienste in einem kleinen Netzwerk von einem Client, auf dem ICS (Internet Connection Sharing) läuft, oder von einem WAP zur Verfügung gestellt werden. Folgende Dienste werden für IPv4 eingesetzt:

- **DHCP** Weist Hosts, die so eingestellt sind, dass sie ihre Konfiguration automatisch erhalten, die IPv4-Adressen zu. Es weist IPv4-Adressen aus einem oder mehreren Bereichen zu und verwaltet die Lease und Erneuerung von IPv4-Adressen. Für Hosts, die nicht DHCP-fähig sind, können Ausschlussbereiche definiert werden, und für spezifische MAC-Adressen (Media Access Control) können statische Zuweisungen vorgenommen werden. DHCP kann auch die IPv4-Adressen von Standardgateways und DNS-Servern liefern.
- **DNS** Löst sowohl lokale Hostnamen als auch vollqualifizierte Domänennamen (Fully Qualified Domain Name, FQDN), beispielsweise *www.contoso.internal*, in IPv4-Adressen auf (und umgekehrt). Ein lokaler DNS-Server kann diese Funktion in seinem eigenen Subnetz wahrnehmen. Wenn Sie zum Beispiel im Eingabeaufforderungsfenster `ping canberra` eingeben, löst DNS den Computernamen *Canberra* in die entsprechende IPv4-Adresse auf. DNS arbeitet auch über das Internet, um die FQDNs von Remotewebsites in ihre IPv4-Adressen aufzulösen. DNS stellt ein verbindungsspezifisches DNS-Suffix für E-Mail-Adressen zur Verfügung. Falls Sie in Ihrem Netzwerk einen E-Mail-Server haben (etwa einen Computer, auf dem Microsoft Exchange Server läuft), ist das verbindungsspezifische DNS-Suffix der Abschnitt der E-Mail-

Adresse hinter dem @-Symbol (beispielsweise *don.hall@tailspintoys.com*). DDNS (Dynamic Domain Name Service) implementiert das Konzept einer dynamischen Datenbank und ermöglicht dynamische Aktualisierungen.



Weitere Informationen Interne und externe Auflösung

Wenn Sie einen Computernamen aus Ihrem internen Netzwerk in eine IPv4-Adresse auflösen (weil Sie beispielsweise **ping canberra** im Eingabeaufforderungsfenster eingegeben haben), liefert der DNS-Dienst in Ihrem WAP oder ICS-Computer die IPv4-Adresse, die diesem Computernamen zugeordnet ist. Müssen Sie dagegen einen FQDN im Internet auflösen (etwa wenn Sie **http://www.contoso.com** in Ihrem Browser eingegeben haben), wird dieser FQDN über das Internet aufgelöst. Bei der Auflösung von FQDNs über das Internet kommen eine DNS-Serverhierarchie und ein iterativer Prozess zum Einsatz. Es ist unwahrscheinlich, dass Sie in Prüfung 70-680 Kenntnisse über iterative DNS-Abfragen unter Beweis stellen müssen. Wenn Sie sich für das Thema interessieren, können Sie sich unter *http://technet.microsoft.com/de-de/library/cc775637.aspx* genauer darüber informieren.

- **APIPA** Konfiguriert ein internes privates Netzwerk, wenn DHCP nicht zur Verfügung steht. Falls Sie ein Netzwerk haben, das keine Verbindung mit anderen Netzwerken besitzt, und möchten, dass die Computer in diesem Netzwerk miteinander kommunizieren, können Sie sie über einen Ethernetswitch verbinden und ihnen erlauben, sich selbst zu konfigurieren. Dafür ist kein DHCP-Dienst erforderlich. APIPA konfiguriert die IPv4-Einstellungen eines Computers mit einer IPv4-Adresse im Bereich von 169.254.0.1 bis 169.254.255.254 mit der Subnetzmaske 255.255.0.0. APIPA konfiguriert kein Standardgateway, weil ein über APIPA konfiguriertes Netzwerk keine IPv4-Pakete in andere Netzwerke sendet oder daraus empfängt.
- **NAT** Erlaubt es, dass viele Geräte in einem privaten Netzwerk über eine einzige öffentliche IPv4-Adresse Zugriff auf das Internet erhalten. NAT übersetzt zwischen den privaten IPv4-Adressen, die in einem lokalen Netzwerk intern benutzt werden, und den öffentlichen Adressen, die im Internet verwendet werden. Wenn Sie eine Anforderung ins Internet senden, indem Sie zum Beispiel eine URL (Uniform Resource Locator) in einem Browser eingeben, müssen die Informationen, die die Antwort bilden (die Webseite), ihren Weg zurück auf Ihren Computer finden, der eine interne IPv4-Adresse in Ihrem LAN (Local Area Network) hat. Normalerweise weist Ihnen Ihr Internetprovider nur eine öffentliche IPv4-Adresse zu, die alle Computer in Ihrem LAN gemeinsam verwenden, wenn sie auf das Internet zugreifen. NAT verwaltet diese Vorgänge und stellt sicher, dass IPv4-Pakete aus dem Internet das richtige Ziel im LAN erreichen.



Weitere Informationen Network Address Translation

Weitere Informationen über NAT finden Sie unter *http://technet.microsoft.com/en-us/library/cc739385.aspx*.

Öffentliche und private IPv4-Adressen

Jedes Gerät im Internet hat eine eindeutige öffentliche IPv4-Adresse, die von keinem anderen Gerät benutzt werden darf. (Ein LAN hat ebenfalls mindestens eine IPv4-Adresse, die im Internet einmalig ist.) Geben Sie beispielsweise eine URL wie *http://www.adatum.com* in Ihrem Webbrowser ein, identifiziert der FQDN *www.adatum.com* einen Webserver mit einer öffentlichen IPv4-Adresse, zum Beispiel 207.46.197.32.

Jede Organisation, die eine Internetpräsenz unterhält, bekommt eine oder mehrere öffentliche IPv4-Adressen zugewiesen, die ausschließlich diese Organisation verwenden kann. Die IANA (Internet Assigned Numbers Authority) vergibt und verwaltet öffentliche IPv4-Adressen über verschiedene Unterorganisationen, etwa RIPE in Europa. Im Fall eines SOHO-Netzwerks weist der Internetprovider eine öffentliche IPv4-Adresse aus einem Bereich zu, den die IANA oder eine ihrer Unterorganisationen dem Internetprovider zugeteilt hat.

Die meisten Organisationen haben nicht genug öffentliche IPv4-Adressen, um jedem Gerät in ihren Netzwerken eine eigene zuzuweisen. Außerdem kann es Sicherheitsprobleme auslösen, wenn Computer im Netzwerk einer Organisation öffentliche IPv4-Adressen haben. Stattdessen verwenden Organisationen private IPv4-Adressen für ihre internen Netzwerke und setzen diese Adressen mit NAT in öffentliche Adressen für den Internetzugriff um.

Private IPv4-Adressen sollten niemals im Internet benutzt werden. Normalerweise ignorieren Router im Internet private IPv4-Adressen. Eine Organisation kann intern einen beliebigen privaten IPv4-Adressbereich verwenden, ohne dafür eine Genehmigung der IANA einholen zu müssen. Weil private IPv4-Adressen nur intern in einer Organisation gelten, können viele Organisationen dieselben IPv4-Adressbereiche verwenden, ohne dass Adresskonflikte entstehen. Die meisten Computer in internen Netzwerken benötigen keine eindeutige öffentliche Adresse. Stattdessen teilen sie sich eine einzige öffentliche Adresse, die ihr LAN identifiziert und die NAT in ihre privaten Adressen umsetzt. Nur Geräte in einem LAN, die eine Internetpräsenz haben (beispielsweise Webserver, E-Mail-Server und DNS-Server), benötigen eine einmalige öffentliche Adresse, die über NAT in ihre interne private Adresse umgesetzt wird.

IANA hat die folgenden drei Blöcke im IPv4-Adressraum für private Netzwerke reserviert:

- 10.0.0.0/8 (10.0.0.1 bis 10.255.255.254)
- 172.16.0.0/12 (172.16.0.1 bis 172.31.255.254)
- 192.168.0.0/16 (192.168.0.1 bis 192.168.255.255)

Außerdem wird auch der APIPA-Bereich 169.254.0.0/16 (169.254.0.1 bis 169.254.255.254) als privat betrachtet, weil diese Adressen niemals im Internet auftauchen sollten. Sie sollten diesen Bereich aber nur für die automatische Zuweisung von IPv4-Adressen durch APIPA in einem isolierten Subnetz verwenden. Setzen Sie diesen Bereich nicht in privaten Netzwerken ein, die ihre Geräte über DHCP oder manuell (statisch) konfigurieren und den Internetzugriff über NAT implementieren.

Die meisten Organisationen verwenden nur einen kleinen Teilbereich des privaten Adressraums. Zum Beispiel enthält das Netzwerk 10.0.0.0/8 über 16 Million Hostadressen, und nur sehr wenige Organisationen benötigen so viele. Ein Unternehmen mit zwei privaten Subnetzen kann beispielsweise die Bereiche 10.0.10.0/24 (10.0.10.1 bis 10.0.10.254) und 10.0.20.0/24 (10.0.20.1 bis 10.0.20.254) für diese Subnetze verwenden. ICS verwendet den Adressbereich 192.168.0.0/24 (192.168.0.1 bis 192.168.0.254), ebenso wie die meisten WAPs.



Hinweis Private Netzwerke – das definitive Dokument

Die exakte Definition eines privaten Netzwerks lautet: ein Netzwerk, das den IPv4-Adressraum aus RFC 1918 verwendet. In Ihrem Beruf als Netzwerkadministrator werden Sie im Lauf der Zeit immer häufiger auf RFCs wie diese zurückgreifen. Sie können diese RFC unter *http://tools.ietf.org/html/rfc1918* lesen.

Herstellen der Verbindung zu einem Netzwerk

Wenn Sie ein Test- oder SOHO-Kabelnetzwerk von Grund auf neu einrichten, beginnen Sie wahrscheinlich mit einem einzigen Computer, der an Ihr Modem angeschlossen ist (über Kabel oder WLAN bei einem WAP), über das eine Verbindung ins Internet möglich wird. Die meisten Netzwerke sind mit dem Internet verbunden, entweder direkt oder über andere Netzwerke. Falls Ihr Netzwerk vollständig isoliert ist und keine Verbindungen ins Internet oder zu anderen LANs hat, reicht es normalerweise aus, wenn sich dieses Netzwerk mit APIPA selbst konfiguriert.

Häufiger kommt es vor, dass Sie einen Computer zu einem vorhandenen Netzwerk hinzufügen (etwa zu einem SOHO- oder kleinen Testnetzwerk). In diesem Fall gibt es üblicherweise schon einen DHCP-Dienst im Netzwerk, sei es auf einem Computer, der ICS zur Verfügung stellt, oder (im Fall eines Drahtlosnetzwerks) in einem WAP. Wenn Sie eine Verbindung ins Internet herstellen, konfiguriert Ihr Internetprovider automatisch Ihre DFÜ- oder DSL-Modemverbindung. Wenn Sie die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing, ICS) einrichten, konfiguriert der Computer in Ihrem Netzwerk, der direkten Zugriff auf das Modem hat, automatisch alle anderen Computer in seinem Subnetz.



Weitere Informationen Gemeinsame Nutzung der Internetverbindung

Weitere Informationen über ICS und ein aufschlussreiches Diagramm finden Sie unter *http://windows.microsoft.com/de-de/windows-vista/Using-ICS-Internet-Connection-Sharing*. Dieser Artikel behandelt Windows Vista, die Informationen gelten aber genauso für Windows 7, wenn Sie »Netzwerkverbindungen verwalten« durch »Adaptereinstellungen ändern« ersetzen.

Die Clientcomputer in einem Netzwerk sind meist so eingerichtet, dass sie ihre IP-Konfigurationen automatisch erhalten. Ist der Computer, den Sie hinzufügen, allerdings ein ICS-Client, müssen Sie das Netzwerk- und Freigabecenter öffnen, auf *Internetoptionen* klicken, auf der Registerkarte *Verbindungen* auf *LAN-Einstellungen* klicken und im Dialogfeld *Einstellungen für lokales Netzwerk* das Kontrollkästchen *Automatische Suche der Einstellungen* deaktivieren. In den Übungen weiter unten in dieser Lektion konfigurieren Sie einen ICS-Computer und einen ICS-Client.

Ob ein Computer richtig konfiguriert ist und seine IPv4-Konfigurationen automatisch erhält, können Sie im Netzwerk- und Freigabecenter überprüfen. Klicken Sie dazu in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*. Klicken Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern*. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit Ihrem Testnetzwerk verbunden ist (meist *LAN-Verbindung*), und wählen Sie den Befehl *Eigenschaften*. Daraufhin öffnet sich das Dialogfeld *Eigenschaften von LAN-Verbindung* (Abbildung 6.2).

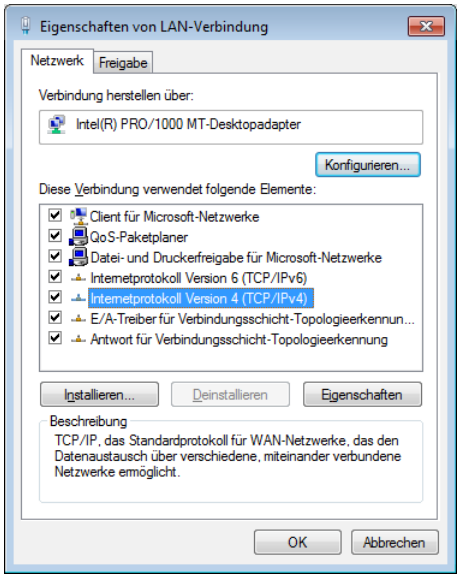


Abbildung 6.2 Dialogfeld *Eigenschaften von LAN-Verbindung*

Wählen Sie in diesem Dialogfeld den Eintrag *Internetprotokoll Version 4 (TCP/IPv4)* aus und klicken Sie dann auf die Schaltfläche *Eigenschaften*. Sofern Sie keine manuelle Konfiguration eingerichtet haben, indem Sie die Option *Folgende IP-Adresse verwenden* ausgewählt haben, müssten Sie feststellen, dass IPv4 für die automatische Konfiguration eingerichtet ist, wie in Abbildung 6.3 zu sehen. Wenn Sie auf die Registerkarte *Alternative Konfiguration* klicken, sehen Sie, dass standardmäßig APIPA benutzt wird, falls keine DHCP-Informationen zur Verfügung stehen.

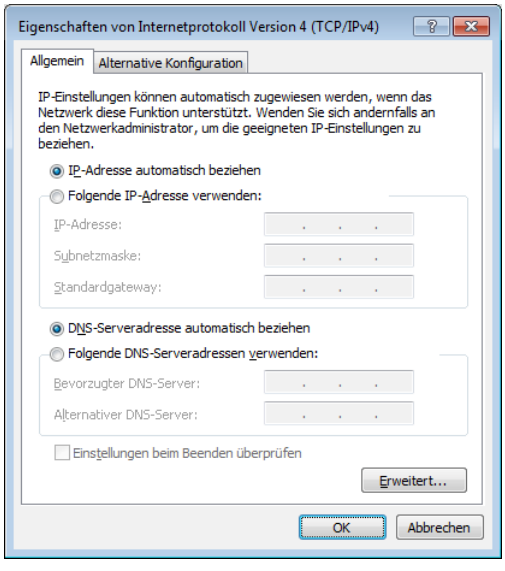


Abbildung 6.3 Automatische IPv4-Konfiguration

Lektion 3 beschreibt die verschiedenen Konfigurationsoptionen und Kombinationen aus Kabel- und Drahtlosverbindungen mit Computern, Modems und WAPs, die beim Einrichten eines SOHO- oder kleinen Testnetzwerks zum Einsatz kommen. Ein Produktivnetzwerk einzurichten, ist viel komplexer. Dabei werden mehrere Firewalls, Umkreisnetzwerke, NAT-Server und so weiter benutzt. Es ist unwahrscheinlich, dass Sie in Prüfung 70-680 Fragen erhalten, zu deren Beantwortung Sie wissen müssen, wie Sie ein vollständig geschütztes Produktivnetzwerk in einem großen Unternehmen einrichten. In dieser Lektion verbinden wir die Computer *Canberra* und *Aberdeen* in einem privaten Kabelnetzwerk. Außerdem verbinden wir (optional) den Computer *Canberra* über WLAN mit einem WAP, der über ein DSL-Modem auf das Internet zugreift (oder es kommt ein Kombigerät zum Einsatz, das WAP und DSL-Modem vereinigt), und konfigurieren auf diesem Computer ICS.

Sie stellen eine Drahtlosverbindung zu einem WAP her (sofern nötig), indem Sie das Netzwerk- und Freigabecenter öffnen (Abbildung 6.4) und auf *Verbindung mit einem Netzwerk herstellen* klicken. Sie können nun einen Eintrag aus der Liste der verfügbaren Netzwerke auswählen. Sie können auch festlegen, dass der Computer immer eine Verbindung zu diesem Netzwerk aufbaut, wenn es in Reichweite ist.

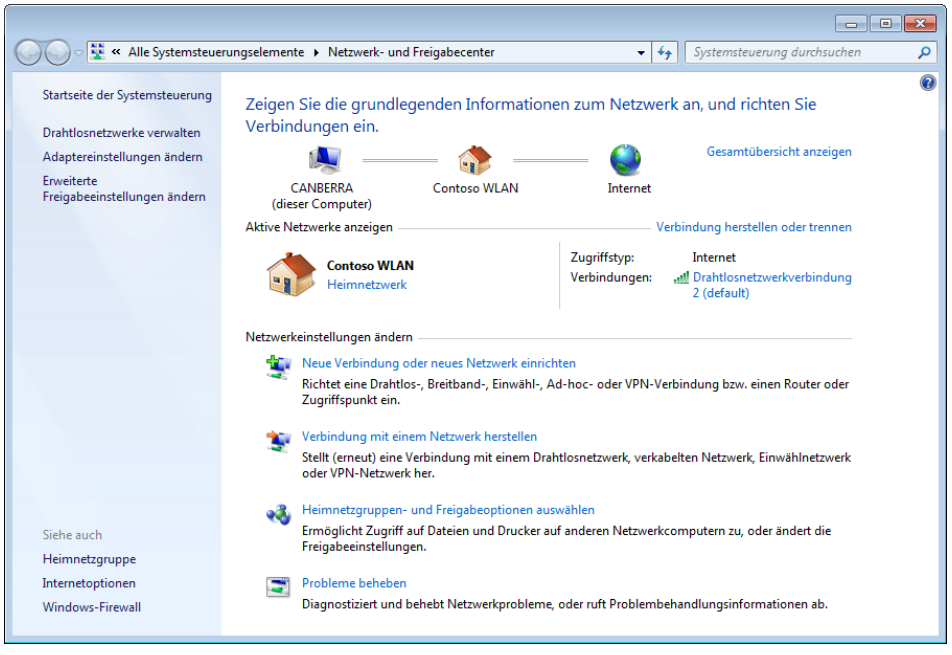

« Alle Systemsteuerungselemente ▸ Netzwerk- und Freigabecenter
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Drahtlosnetzwerke verwalten
Adaptereinstellungen ändern
Erweiterte Freigabeeinstellungen ändern
Zeigen Sie die grundlegenden Informationen zum Netzwerk an, und richten Sie Verbindungen ein.
Gesamtübersicht anzeigen
CANBERRA (dieser Computer)
Contoso WLAN
Internet
Aktive Netzwerke anzeigen
Verbindung herstellen oder trennen
Contoso WLAN
Heimnetzwerk
Zugriffstyp: Internet
Verbindungen: Drahtlosnetzwerkverbindung 2 (default)
Netzwerkeinstellungen ändern
Neue Verbindung oder neues Netzwerk einrichten
Richtet eine Drahtlos-, Breitband-, Einwähl-, Ad-hoc- oder VPN-Verbindung bzw. einen Router oder Zugriffspunkt ein.
Verbindung mit einem Netzwerk herstellen
Stellt (erneut) eine Verbindung mit einem Drahtlosnetzwerk, verkabelten Netzwerk, Einwählnetzwerk oder VPN-Netzwerk her.
Heimnetzgruppen- und Freigabeoptionen auswählen
Ermöglicht Zugriff auf Dateien und Drucker auf anderen Netzwerkcomputern zu, oder ändert die Freigabeeinstellungen.
Probleme beheben
Diagnostiziert und behebt Netzwerkprobleme, oder ruft Problembehandlungsinformationen ab.
Siehe auch
Heimnetzgruppe
Internetoptionen
Windows-Firewall

Abbildung 6.4 Das Netzwerk- und Freigabecenter



Hinweis Unkonfigurierte WAPs

Abbildung 6.4 zeigt, dass der Computer *Canberra* mit einem noch unkonfigurierten WAP verbunden ist. Unkonfigurierte WAPs tragen normalerweise den Namen *default*, haben das Kennwort »admin« und erlauben es einem Clientcomputer, eine Verbindung dazu herzustellen. Dieser WAP ist noch unkonfiguriert, weil die WAP-Konfiguration erst in Lektion 3 beschrieben wird. Sie sollten Ihren WAP immer konfigurieren, ansonsten öffnen Sie eine schwere Sicherheitslücke.

Einrichten einer IPv4-Konfiguration

Im Dialogfeld *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)*, das in Abbildung 6.3 weiter oben gezeigt ist, können Sie *Folgende IP-Adresse verwenden* auswählen und eine statische IPv4-Adresse, eine Subnetzmaske und ein Standardgateway eingeben. Sie können außerdem *Folgende DNS-Serveradresse verwenden* auswählen und die IPv4-Adresse eines DNS-Servers sowie eines alternativen DNS-Servers eingeben, den der Client benutzt, wenn der erste nicht verfügbar ist. Wenn Sie auf *Erweitert* klicken, haben Sie die Möglichkeit, weitere DNS-Server hinzuzufügen. Sie können auch die IPv4-Adressen von WINS-Servern (Windows Internet Naming Service) angeben, wenn Sie für die NetBIOS-Namensauflösung gebraucht werden.

Viele Administratoren verwenden stattdessen lieber das Befehlszeilentool Netsh in einer Eingabeaufforderung mit erhöhten Rechten. Wollen Sie beispielsweise die Schnittstelle *LAN-Verbindung* mit der IPv4-Adresse 10.0.0.11, der Subnetzmaske 255.255.255.0 und dem Standardgateway 10.0.0.11 konfigurieren, geben Sie folgenden Befehl ein:

```
netsh interface ipv4 set address "LAN-Verbindung" static 10.0.0.11 255.255.255.0 10.0.0.11
```

Und der folgende Befehl legt als DNS-Serveradresse 10.0.0.11 fest:

```
netsh interface ipv4 set dnsservers "LAN-Verbindung" static 10.0.0.11
```

Wenn die Schnittstelle ihre IPv4-Konfiguration automatisch (dynamisch) erhalten soll, verwenden Sie diese Befehle:

```
netsh interface ipv4 set address name="LAN-Verbindung" source=dhcp
netsh interface ipv4 set dnsservers name="LAN-Verbindung" source=dhcp
```

In den Übungen weiter unten in dieser Lektion verwenden Sie sowohl das Dialogfeld *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)* als auch Netsh, um eine Schnittstelle zu konfigurieren.



Hinweis Syntax von Netsh

Aus Gründen der Abwärtskompatibilität können Sie statt `netsh interface ipv4` auch den Befehl `netsh interface ip` verwenden. Für die IPv6-Befehle von Netsh müssen Sie dagegen `ipv6` angeben. Beachten Sie auch, dass der Schnittstellenname bei statischen Einstellungen einfach als `LAN-Verbindung` angegeben wird. Die Syntax `name="LAN-Verbindung"` wird akzeptiert, ist aber nicht nötig. Bei einer dynamischen Konfiguration müssen Sie dagegen `name="LAN-Verbindung"` verwenden.

Beseitigen von Netzwerkproblemen

Als IT-Experte bekommen Sie es häufig mit dem Problem zu tun, dass Computer nicht untereinander, mit anderen internen Netzwerken innerhalb Ihrer Organisation oder mit dem Internet kommunizieren können. In diesem Abschnitt lernen Sie allgemeine Problembehandlungswerkzeuge kennen, die Ihnen bei der Analyse von Netzwerkproblemen helfen. Eines dieser Werkzeuge ist die Windows-Netzwerkdiagnose.

Grundlegende Problembehandlung

Verbindungsprobleme können viele Ursachen haben. In Kabelnetzwerken kann ein Kabel defekt oder nicht richtig eingesteckt sein. Schnittstellen, die ihre IP-Konfigurationen dynamisch beziehen sollten, können für eine statische Konfiguration eingerichtet sein. Wo zwei

oder mehr Schnittstellen eine Netzwerkbrücke bilden, können eine oder mehrere Schnittstellen von der Brücke entfernt worden sein. In einer Unternehmensumgebung ist vielleicht ein DHCP- oder DNS-Server oder sogar ein Domänencontroller ausgefallen (allerdings sollte in diesem Fall ein Failovermechanismus zum Einsatz kommen). Oder eine Firewall ist falsch konfiguriert.

In einem kleinen Netzwerk kann ICS falsch oder überhaupt nicht eingerichtet sein. Der WAP eines Fremdherstellers kann zu einem Kabelnetzwerk hinzugefügt worden sein, damit Drahtloscomputer eine Verbindung herstellen können, aber der Computer, der vorher ICS zur Verfügung gestellt hat, wurde nicht so umkonfiguriert, dass er seine Einstellungen vom WAP bezieht. Ein WAP, eine Netzwerkkarte oder ein Modem kann defekt sein. Ihr Internetprovider kann einen Ausfall haben. Neu installierte Software kann Ihre Verbindungseigenschaften verändert haben. Die Liste ist praktisch endlos.

Zuerst sollten Sie immer die offensichtlichen Punkte überprüfen. Beginnen Sie beim Netzwerk und stellen Sie sicher, dass keine Kabel ganz oder teilweise herausgezogen wurden, sodass unzuverlässige Verbindungen entstehen. Stellen Sie sicher, dass alle Lämpchen an Modem, WAP und Netzwerkschnittstellen leuchten, wenn sie sollten, und blinken, wenn sie sollten. Falls ein Gerät kein Lebenszeichen von sich gibt, sollten Sie prüfen, ob sein Netzteil an die Steckdose und das Gerät angeschlossen ist. Überprüfen Sie alle roten LEDs. Ein rotes Licht bedeutet nicht immer einen Fehler, aber Rot steht meist für ein Warnzeichen.

Falls Sie Probleme mit Drahtlosverbindungen haben, können Sie versuchsweise den WAP ausschalten. Schalten Sie dann alle Computer aus, die über Ethernetkabel mit dem WAP verbunden sind, am besten auch gleich Ihre Drahtloscomputer. Warten Sie einige Minuten, schalten Sie den WAP wieder an und starten Sie die Computer neu. Falls Sie das Modem im Verdacht haben, sollten Sie das Modem, den WAP und alle Netzwerkcomputer ausschalten und dann wieder in dieser Reihenfolge einschalten. Überprüfen Sie die Einstellung des WAPs.

Überprüfen der Verbindung zwischen zwei Computern

Bevor Sie die Tools verwenden, die Windows 7 zum Überprüfen der Computer-zu-Computer-Konnektivität zur Verfügung stellt, sollten Sie erst einmal sicherstellen, dass der Computer, zu dem Sie eine Verbindung herstellen wollen, überhaupt eingeschaltet ist. In einem Kabelnetzwerk müssen Sie sicherstellen, dass er ans Netzwerk angeschlossen ist. Falls Sie ICS verwenden, müssen Sie auch sicherstellen, dass der ICS-Computer eingeschaltet ist und läuft. Andernfalls kann keiner der anderen Computer eine Verbindung zum Internet herstellen. Wenn die Computer in Ihrem Netzwerk ihre IPv4-Verbindungsdaten von einem WAP bekommen, müssen Sie sicherstellen, dass der WAP eingeschaltet und mit dem Modem verbunden ist.

Damit ein Windows 7-Computer eine Verbindung zu anderen Computern in einem LAN herstellen kann, muss die Netzwerkerkennung auf Quell- und Zielcomputer aktiviert sein. Die Netzwerkerkennung ist standardmäßig aktiviert, aber falls beim Zugriff auf andere Computer Probleme auftreten, sollten Sie diese Einstellung überprüfen, indem Sie im Netzwerk- und Freigabecenter auf *Erweiterte Freigabeeinstellungen ändern* klicken. Abbildung 6.5 zeigt das Dialogfeld *Erweiterte Freigabeeinstellungen*.

Treten bei einer Netzwerkverbindung sporadisch Probleme auf, reicht es manchmal aus, den Gerätetreiber für den Netzwerkanschluss zu deaktivieren und dann wieder zu aktivieren. Hilft das nicht, ist der Gerätetreiber möglicherweise beschädigt oder veraltet. Vielleicht wurde er auch vor Kurzem durch einen neuen Treiber ersetzt, der Kompatibilitätsprobleme

verursacht. Kapitel 4, »Verwalten von Geräten und Datenträgern«, beschreibt genauer, wie Sie Treiber aktualisieren oder deinstallieren, ihre Vorversion wiederherstellen und eine Problembehandlung durchführen.

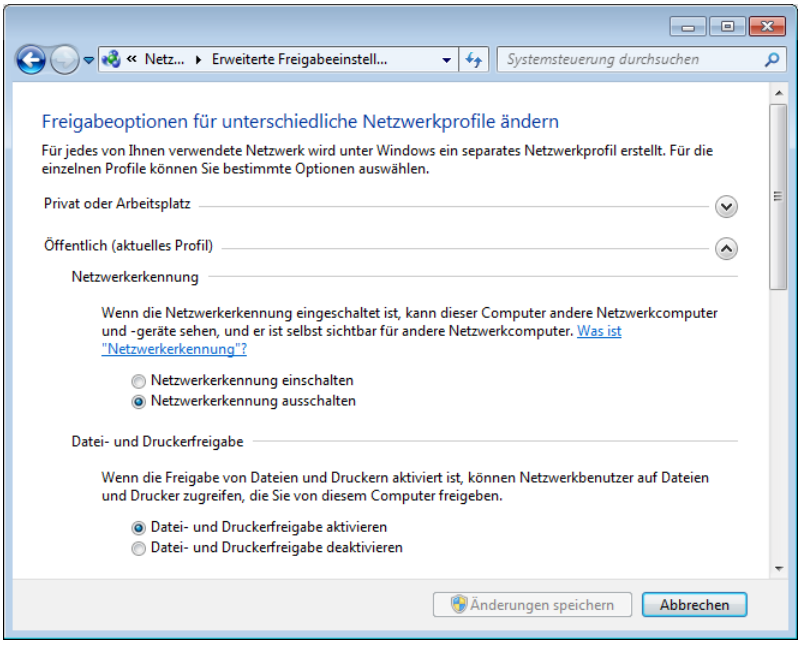

« Netz... ▸ Erweiterte Freigabeeinstell...
Systemsteuerung durchsuchen
Freigabeoptionen für unterschiedliche Netzwerkprofile ändern
Für jedes von Ihnen verwendete Netzwerk wird unter Windows ein separates Netzwerkprofil erstellt. Für die einzelnen Profile können Sie bestimmte Optionen auswählen.
Privat oder Arbeitsplatz
Öffentlich (aktuelles Profil)
Netzwerkerkennung
Wenn die Netzwerkerkennung eingeschaltet ist, kann dieser Computer andere Netzwerkcomputer und -geräte sehen, und er ist selbst sichtbar für andere Netzwerkcomputer. Was ist "Netzwerkerkennung"?
Netzwerkerkennung einschalten
Netzwerkerkennung ausschalten
Datei- und Druckerfreigabe
Wenn die Freigabe von Dateien und Druckern aktiviert ist, können Netzwerkbenutzer auf Dateien und Drucker zugreifen, die Sie von diesem Computer freigeben.
Datei- und Druckerfreigabe aktivieren
Datei- und Druckerfreigabe deaktivieren
Änderungen speichern
Abbrechen

Abbildung 6.5 Das Dialogfeld *Erweiterte Freigabeeinstellungen*

Problembehandlung für die IP-Konfiguration

Befehlszeilentools für die Problembehandlung der IP-Konfiguration gibt es schon lange und sie sind weithin bekannt. Das Tool *Ping* ist immer noch eines der meistbenutzten Werkzeuge, allerdings blockieren immer mehr Firewalls ICMP-Echoanforderungen (Internet Control Message Protocol). Aber auch wenn Sie nicht durch eine Firewall im Netzwerk Ihrer Organisation kommen, ist Ping nach wie vor nützlich. Sie können überprüfen, ob IPv4 auf einem Computer funktioniert, indem Sie **ping 127.0.0.1** eingeben. Anschließend können Sie die IPv4-Adresse des Computers anpingen. Diese Adresse finden Sie über den Befehl `ipconfig` heraus. Falls Ihr Computer mehrere Schnittstellen zu einer Netzwerkbrücke zusammenfasst, können Sie die IPv4-Adresse der Netzwerkbrücke anpingen. Wenn Sie sichergestellt haben, dass Sie Ihren Computer über eine IPv4-Adresse anpingen können, sollten Sie prüfen, ob DNS intern in Ihrem Netzwerk arbeitet (sofern Sie mit einem DNS-Server oder einem WAP verbunden sind oder ICS in Ihrem Netzwerk konfiguriert haben). Pingen Sie dazu den Namen Ihres Computers an, indem Sie beispielsweise **ping canberra** eingeben. Auch wenn DNS in Ihrem System nicht implementiert ist, funktioniert `ping canberra` trotzdem, weil die verbindungslokale IPv6-Adresse automatisch aufgelöst wird.



Weitere Informationen Netzwerkbrücken

Weitere Informationen über Netzwerkbrücken finden Sie unter *http://technet.microsoft.com/de-de/library/cc781097.aspx*. Dieser Artikel ist zwar schon ziemlich alt (er behandelt Windows Server 2003), erklärt das Konzept aber sehr verständlich und enthält mehrere aussagekräftige Diagramme. Einen neueren Artikel (allerdings nicht über Windows 7 und nur in englischer Sprache) finden Sie unter *http://technet.microsoft.com/en-us/library/cc748895.aspx*. Er enthält auch Informationen über ICS.

Sie können für die Problembehandlung auch das Tool Ipconfig einsetzen. Durch Eingabe von **ipconfig /all** bekommen Sie Konfigurationsinformationen zu allen Schnittstellen aufgelistet. Abbildung 6.6 zeigt die Ausgabe des Befehls `ipconfig /all`. Der Computer, dessen Konfiguration hier gezeigt wird, ist ein WLAN-fähiges Notebook, das in einem kleinen Testnetzwerk betrieben wird. Er ruft seine Konfiguration über DHCP vom WAP eines anderen Herstellers ab, der die IPv4-Adresse 192.168.123.254 hat. Der WAP stellt auch interne DNS-Dienste zur Verfügung. Die Auflösung von FQDNs wie *www.contoso.com* wird allerdings vom DNS-Server des Internetproviders mit der öffentlichen IPv4-Adresse 194.168.4.100 erledigt.

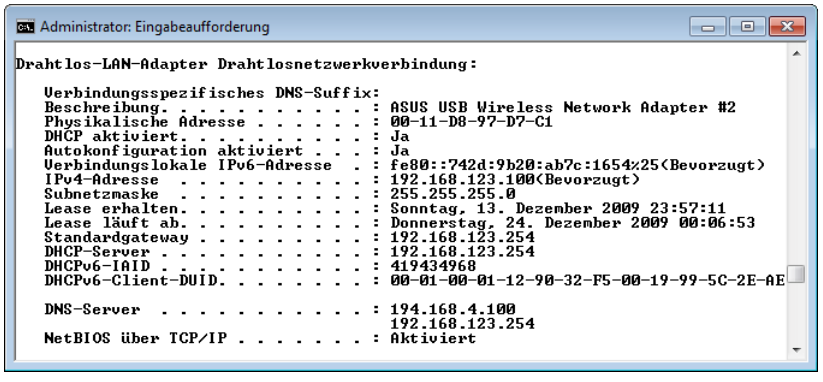

Administrator: Eingabeaufforderung
Drahtlos-LAN-Adapter Drahtlosnetzwerkverbindung:
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : ASUS USB Wireless Network Adapter #2
Physikalische Adresse . . . . . : 00-11-D8-97-D7-C1
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . : fe80::742d:9b20:ab7c:1654%25(Bevorzugt)
IPv4-Adresse . . . . . : 192.168.123.100(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Sonntag, 13. Dezember 2009 23:57:11
Lease läuft ab. . . . . : Donnerstag, 24. Dezember 2009 00:06:53
Standardgateway . . . . . : 192.168.123.254
DHCP-Server . . . . . : 192.168.123.254
DHCPv6-IAID . . . . . : 419434968
DHCPv6-Client-DUID. . . . . : 00-01-00-01-12-90-32-F5-00-19-99-5C-2E-AE
DNS-Server . . . . . : 194.168.4.100
192.168.123.254
NetBIOS über TCP/IP . . . . . : Aktiviert

Abbildung 6.6 Ausgabe von `ipconfig /all` bei einem WLAN-fähigen Notebook in einem Testnetzwerk

Wenn Sie Verbindungsprobleme mithilfe des Befehls `ipconfig /all` analysieren, sollten Sie nach Adressen im APIPA-Bereich 169.254.0.1 bis 169.254.255.254 Ausschau halten. Wenn sich Ihr Computer in einem Netzwerk befindet, das nicht vollständig isoliert ist, und seine Konfiguration über DHCP erhält, bedeutet eine APIPA-Adresse, dass ein Verbindungsfehler vorliegt.

Wenn es gelingt, Ihren Computer erfolgreich anhand seines Namens und der IPv4-Adresse anzupingen, können Sie als Nächstes versuchen, andere Arbeitsstationen in Ihrem Netzwerk anhand ihrer IPv4-Adressen und Computernamen anzupingen. Schließlich sollten Sie überprüfen, ob Sie Ihr Standardgateway von allen Computern im Netzwerk aus mit Ping erreichen. In einem kleinen Netzwerk können Sie dann die Konnektivität zu Ihrem Internetprovider testen, indem Sie den DNS-Server des Internetproviders anpingen. In einem großen Unternehmensnetzwerk können Sie die DNS-Server und Domänencontroller (üblicherweise dieselben Server) sowie Computer in anderen Subnetzen anpingen.

Falls Sie einen Computer in Ihrem Netzwerk nicht anpingen können, um die Konnektivität zu testen, sollten Sie überprüfen, ob Ihre internen Firewalls ICMP blockieren. Besteht das Problem weiter, obwohl die Firewalls umkonfiguriert oder deaktiviert wurden (vergessen Sie nicht, sie hinterher wieder zu aktivieren), sollten Sie auf dem Computer, den Sie nicht erreichen können, Ipconfig ausführen, um seine IP-Einstellungen zu überprüfen.

Schnelltest

- Sie haben einen gebrauchten Computer gekauft und schließen ihn an ein Hybridnetzwerk an, das seine Konfiguration mithilfe von DHCP von einem WAP bezieht. Der Computer ist nicht WLAN-fähig, daher stecken Sie ihn an einen Ethernetswitch im WAP an und schalten ihn ein. Er kann nicht auf das Internet zugreifen. Mit dem Tool Ipconfig stellen Sie fest, dass der Computer die IP-Adresse 10.1.10.231 hat. Sie wissen, dass der WAP einwandfrei funktioniert und die Ethernetverbindung in Ordnung ist. Was sollten Sie als Nächstes prüfen?

Antwort zum Schnelltest

- Überprüfen Sie, ob der Computer so eingerichtet ist, dass er seine IPv4-Konfiguration dynamisch bezieht. Er wurde nicht mit DHCP-Informationen aus dem WAP konfiguriert, sein Vorbesitzer hat ihn daher wohl mit der statischen Adresse 10.1.10.231 konfiguriert. Sie müssen den Computer so konfigurieren, dass er seine IPv4-Einstellungen dynamisch bezieht.

Wenn Sie die IP-Einstellungen für einen Clientcomputer in Ihrem Netzwerk umkonfigurieren wollen, können Sie ihn einfach neu starten. Ist das zu unbequem, können Sie mit den Befehlen `ipconfig /release`, gefolgt von `ipconfig /renew`, die alte Konfiguration freigeben und eine neue anfordern. (Theoretisch müsste `ipconfig /renew` ausreichen, aber es ist sicherer, immer beide Befehle zu verwenden.) Wenn Sie die Konfiguration eines Computers erneuern, registriert er seine neuen Einstellungen nicht immer sofort in DNS, daher kann es sein, dass Sie ihn nicht über seinen Computernamen anpingen können. In diesem Fall erzwingt `ipconfig /registerdns` eine Registrierung. Beachten Sie, dass Sie diese Befehle in einer Eingabeaufforderung mit erhöhten Rechten ausführen müssen.

Wenn Sie versuchen, von einem Client aus einen Computer anhand seines Namens anzupingen oder auf eine Website zuzugreifen, DNS den Computernamen oder die URL aber nicht auflösen kann, wird die Information, dass die Auflösung fehlgeschlagen ist, in einem Cache des Clients gespeichert. Wenn Sie dieselbe Operation erneut versuchen, versucht der Client gar nicht erst, die Namensauflösung durchzuführen, sondern verwendet die zwischengespeicherten Informationen, sodass die Anforderung erneut fehlschlägt. Das wird als »negative Zwischenspeicherung« (negative caching) bezeichnet. Möglicherweise ist die Namensauflösung aber nur aufgrund eines temporären Fehlers im internen oder externen DNS-Dienst fehlgeschlagen. Obwohl DNS jetzt funktioniert, werden Computername oder FQDN nicht in eine IPv4-Adresse aufgelöst, weil sich die Informationen noch im Zwischenspeicher befinden. Das Problem löst sich nach etwa 30 Minuten von selbst, weil der DNS-Auflösungscache eines Clients regelmäßig gelöscht wird. Falls Sie allerdings nicht so lange warten wollen, können Sie das Problem sofort beseitigen, indem Sie den DNS-Cache mit dem Befehl **ipconfig /flushdns** leeren.



Hinweis Das Befehlszeilenargument */allcompartments*

Wenn Sie den Befehl `ipconfig` mit dem Befehlszeilenargument `/allcompartments` aufrufen, wird der Befehl auf alle Schnittstellen angewendet. Beispielsweise lauten die Befehle dann `ipconfig /allcompartments /all` oder `ipconfig /allcompartments /renew`.

Wenn Sie den Weg eines IP-Pakets durch ein Internetzwerk (eine Reihe von Netzwerken oder Hops) verfolgen wollen, können Sie das Tool *Tracert* verwenden. Es listet auf, welchen Pfad das Paket nimmt und welche Verzögerungen bei jedem Abschnitt (Hop) auftreten. Sie rufen das Tool beispielsweise mit `tracert 194.168.4.100` auf. Sie können mit Tracert den Pfad zu einer Website verfolgen, indem Sie `tracert -d www.contoso.com` ausführen. Das Flag `-d` verhindert, dass das Tool IPv4-Adressen in Hostnamen auflöst, was die Ausführung des Befehls deutlich beschleunigt. Das Tool *Pathping* (beispielsweise `pathping www.contoso.com`) verfolgt eine Route ganz ähnlich wie Tracert, liefert aber ausführlichere Statistiken über jeden Abschnitt.

Arbeiten mit der Windows-Netzwerkdiagnose

Sie sollten sich unbedingt eine gute Technik aneignen, um grundlegende Fehler zu finden. Haben Sie die grundlegenden Punkte einmal überprüft, stellt Windows 7 automatisierte Hilfe in Form der Windows-Netzwerkdiagnose zur Verfügung.

Sie greifen auf die automatisierte Windows-Netzwerkdiagnose zu, wenn die Verbindung zu einer Website im Internet nicht hergestellt werden kann. Die daraufhin im Browser angezeigte Webseite enthält einen direkten Link zu diesem Tool (Abbildung 6.7). Sie brauchen lediglich auf *Diagnose von Verbindungsproblemen* zu klicken.

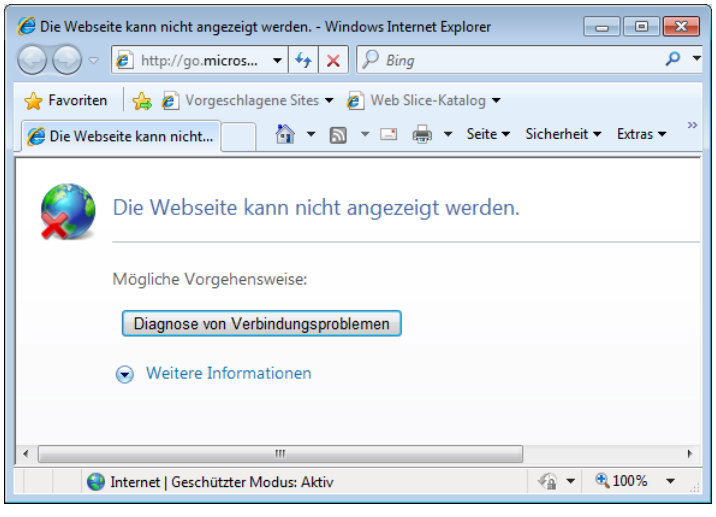


Abbildung 6.7 Der Link *Diagnose von Verbindungsproblemen*

Sie können die Windows-Netzwerkdiagnose auch starten, indem Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern* klicken, mit der rechten Maustaste auf die Schnittstelle klicken, bei der Probleme auftreten, und den Befehl *Diagnose* wählen. Oder Sie starten das Tool im Netzwerk- und Freigabecenter, indem Sie auf das rote X klicken, das auf ein Problem hinweist; dieses Symbol erscheint auf der Verbindungslinie zwischen Ihrem

Computer und dem Netzwerk beziehungsweise zwischen Ihrem Netzwerk und dem Internet. Unabhängig davon, auf welche Weise Sie das Tool starten, führt es automatisch eine Diagnose aus und bietet (sofern möglich) Lösungsvorschläge an. In Abbildung 6.8 sehen Sie, dass der Administrator es versäumt hat, den grundlegenden Prinzipien zu folgen: Er hat nicht geprüft, ob das Ethernetkabel angeschlossen ist.

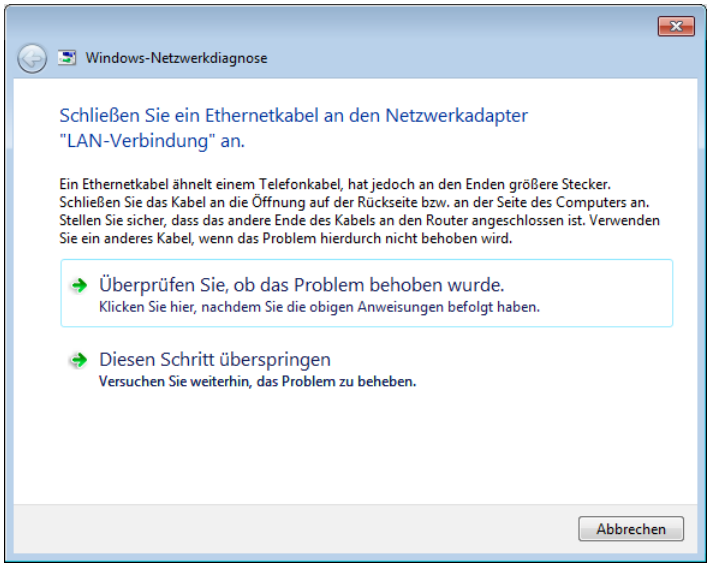

Windows-Netzwerkdiagnose
Schließen Sie ein Ethernetkabel an den Netzwerkadapter "LAN-Verbindung" an.
Ein Ethernetkabel ähnelt einem Telefonkabel, hat jedoch an den Enden größere Stecker. Schließen Sie das Kabel an die Öffnung auf der Rückseite bzw. an der Seite des Computers an. Stellen Sie sicher, dass das andere Ende des Kabels an den Router angeschlossen ist. Verwenden Sie ein anderes Kabel, wenn das Problem hierdurch nicht behoben wird.
Überprüfen Sie, ob das Problem behoben wurde.
Klicken Sie hier, nachdem Sie die obigen Anweisungen befolgt haben.
Diesen Schritt überspringen
Versuchen Sie weiterhin, das Problem zu beheben.
Abbrechen

Abbildung 6.8 Fehlerdiagnose

Weitere Diagnoseoptionen stehen zur Verfügung, wenn Sie im Netzwerk- und Freigabecenter auf *Probleme beheben* klicken (Abbildung 6.9). Die meisten dieser Tools sind aber lediglich ein anderer Weg, auf die Windows-Netzwerkdiagnose zuzugreifen.

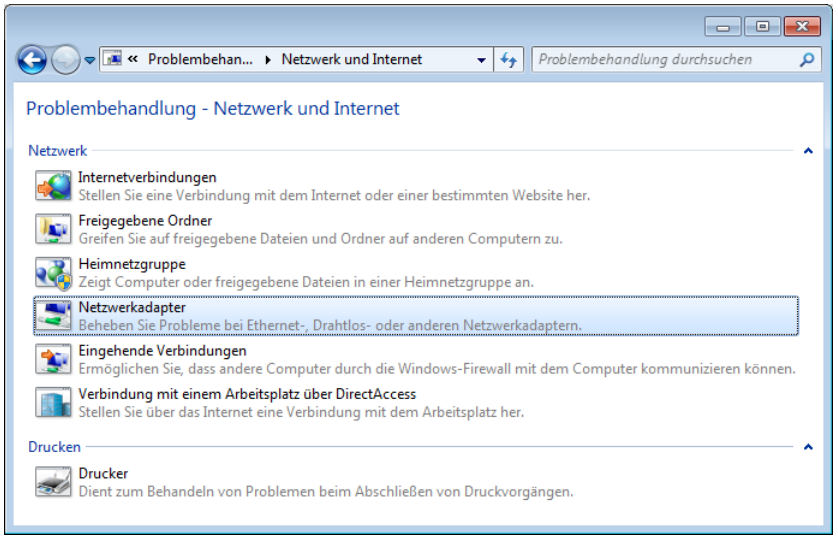

« Problembehan... ▸ Netzwerk und Internet
Problembehandlung durchsuchen
Problembehandlung - Netzwerk und Internet
Netzwerk
Internetverbindungen
Stellen Sie eine Verbindung mit dem Internet oder einer bestimmten Website her.
Freigegebene Ordner
Greifen Sie auf freigegebene Dateien und Ordner auf anderen Computern zu.
Heimnetzgruppe
Zeigt Computer oder freigegebene Dateien in einer Heimnetzgruppe an.
Netzwerkadapter
Beheben Sie Probleme bei Ethernet-, Drahtlos- oder anderen Netzwerkadaptern.
Eingehende Verbindungen
Ermöglichen Sie, dass andere Computer durch die Windows-Firewall mit dem Computer kommunizieren können.
Verbindung mit einem Arbeitsplatz über DirectAccess
Stellen Sie über das Internet eine Verbindung mit dem Arbeitsplatz her.
Drucken
Drucker
Dient zum Behandeln von Problemen beim Abschließen von Druckvorgängen.

Abbildung 6.9 Tools für die Problembehandlung

Konfigurieren von Netzwerkeinstellungen in der Windows-Firewall

Kapitel 7, »Windows-Firewall und Remoteverwaltung«, beschreibt Firewalls und ihre Konfiguration im Detail. Dieses Kapitel enthält daher nur eine kurze Übersicht und behandelt Firewalleinstellungen nur im Zusammenhang mit Netzwerkkonnektivität und erklärt, wie Sie diese Konnektivität testen und reparieren. Die Standardeinstellungen in der Windows-Firewall und der Windows-Firewall mit erweiterter Sicherheit (Windows Firewall with Advanced Security, WFAS) sind vernünftig. Viele Probleme können Sie daher beseitigen, indem Sie einfach die Standardeinstellungen wiederherstellen.

Die Windows-Firewall ist in Windows 7 standardmäßig aktiviert. Sie blockiert jeglichen eingehenden Verkehr, der nicht die Kriterien erfüllt, für die Ausnahmen definiert sind. Sie konfigurieren eine Ausnahme, um einem Programm zu erlauben, Informationen in beiden Richtungen durch die Firewall zu übertragen. Sie können einem Programm auch die Kommunikation durch die Firewall erlauben, indem Sie Ports öffnen. Die Windows-Firewall erlaubt in öffentlichen und privaten Netzwerken standardmäßig den Kernnetzwerkkomponenten die Kommunikation. Wie in Abbildung 6.10 zu sehen, werden die Firewallregeln für das Kernnetzwerk gebraucht, um zuverlässige IPv4- und IPv6-Verbindungen zu gewährleisten. Diese Regeln erlauben allerdings keine ICMPv4- oder ICMPv6-Echoanforderungen; die Firewall blockiert also Ping-Befehle.

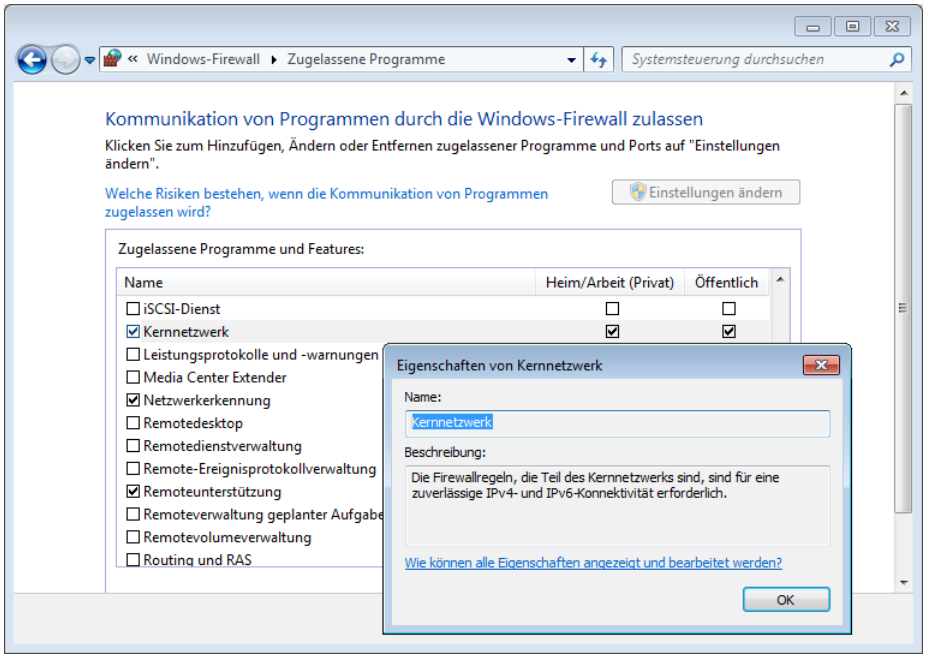


Abbildung 6.10 Firewallregeln für das Kernnetzwerk

Sie greifen auf die Windows-Firewall zu, indem Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows-Firewall* klicken. Im linken Fensterabschnitt können Sie die Firewall ein- oder ausschalten und die Benachrichtigungseinstellungen ändern. Sie können auch auf *Erweiterte Einstellungen* klicken, um auf die Windows-Firewall mit erweiterter Sicherheit zuzugreifen.

Abbildung 6.11 zeigt die eingehenden Regeln für das Kernnetzwerk in der Konsole *Windows-Firewall mit erweiterter Sicherheit*. Die ausgehenden Regeln, die zum Kernnetzwerk gehören, sehen Sie in Abbildung 6.12.

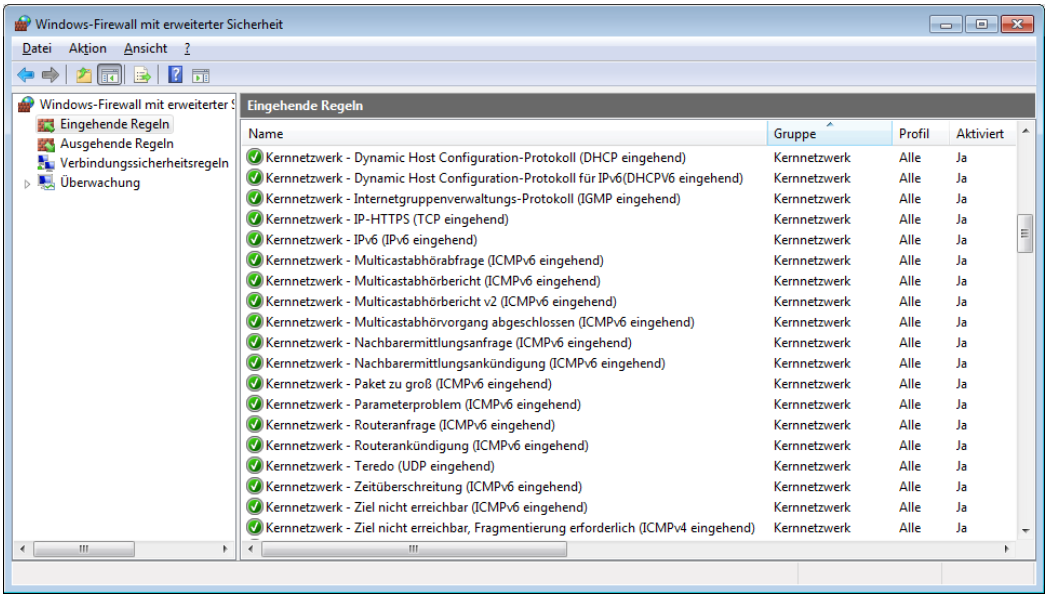

Windows-Firewall mit erweiterter Sicherheit
Datei Aktion Ansicht ?
Windows-Firewall mit erweiterter S
Eingehende Regeln
Ausgehende Regeln
Verbindungssicherheitsregeln
Überwachung
Eingehende Regeln
Name Gruppe Profil Aktiviert
Kernnetzwerk - Dynamic Host Configuration-Protokoll (DHCP eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Dynamic Host Configuration-Protokoll für IPv6(DHCPV6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Internetgruppenverwaltungs-Protokoll (IGMP eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - IP-HTTPS (TCP eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - IPv6 (IPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Multicastabhörabfrage (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Multicastabhörbericht (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Multicastabhörbericht v2 (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Multicastabhörvorgang abgeschlossen (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Nachbarermittlungsanfrage (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Nachbarermittlungsankündigung (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Paket zu groß (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Parameterproblem (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Routeranfrage (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Routerankündigung (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Teredo (UDP eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Zeitüberschreitung (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Ziel nicht erreichbar (ICMPv6 eingehend) Kernnetzwerk Alle Ja
Kernnetzwerk - Ziel nicht erreichbar, Fragmentierung erforderlich (ICMPv4 eingehend) Kernnetzwerk Alle Ja

Abbildung 6.11 Eingehende Regeln in der Konsole *Windows-Firewall mit erweiterter Sicherheit*

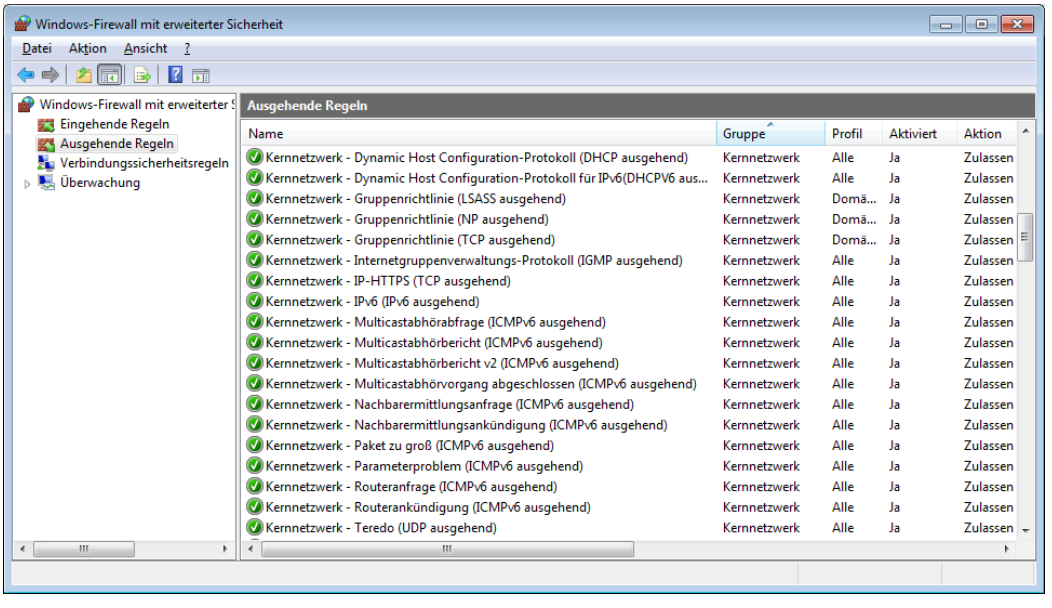

Windows-Firewall mit erweiterter Sicherheit
Datei Aktion Ansicht ?
Windows-Firewall mit erweiterter S
Eingehende Regeln
Ausgehende Regeln
Verbindungssicherheitsregeln
Überwachung
Ausgehende Regeln
Name Gruppe Profil Aktiviert Aktion
Kernnetzwerk - Dynamic Host Configuration-Protokoll (DHCP ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Dynamic Host Configuration-Protokoll für IPv6(DHCPV6 aus... Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Gruppenrichtlinie (LSASS ausgehend) Kernnetzwerk Domä... Ja Zulassen
Kernnetzwerk - Gruppenrichtlinie (NP ausgehend) Kernnetzwerk Domä... Ja Zulassen
Kernnetzwerk - Gruppenrichtlinie (TCP ausgehend) Kernnetzwerk Domä... Ja Zulassen
Kernnetzwerk - Internetgruppenverwaltungs-Protokoll (IGMP ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - IP-HTTPS (TCP ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - IPv6 (IPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Multicastabhörabfrage (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Multicastabhörbericht (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Multicastabhörbericht v2 (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Multicastabhörvorgang abgeschlossen (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Nachbarermittlungsanfrage (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Nachbarermittlungsankündigung (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Paket zu groß (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Parameterproblem (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Routeranfrage (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Routerankündigung (ICMPv6 ausgehend) Kernnetzwerk Alle Ja Zulassen
Kernnetzwerk - Teredo (UDP ausgehend) Kernnetzwerk Alle Ja Zulassen

Abbildung 6.12 Ausgehende Regeln in der Konsole *Windows-Firewall mit erweiterter Sicherheit*

Diese Regeln erlauben bestimmte Verkehrsarten, die nötig sind, damit Windows 7 die entsprechenden Funktionen ausführen kann. Die Verwendung des Tools Ping wird dadurch aber nicht ermöglicht.

Wenn Sie Verbindungsprobleme haben, die beseitigt sind, sobald Sie die Windows-Firewall deaktivieren, sollten Sie sich Ihre Firewalleinstellungen ansehen. In manchen Fällen lassen sich die unmittelbaren Probleme dadurch lösen, dass Sie die Standardeinstellungen wiederherstellen, das ist aber ein sehr grober Ansatz. Schließlich wurden die Einstellungen sehr wahrscheinlich mit Absicht geändert. Sie müssen das Problem also genauer untersuchen. Kapitel 7 beschreibt, wie Sie dabei vorgehen.

Ein Beispiel: Auch wenn Sie die Standardeinstellungen wiederherstellen, können Sie Verbindungen in Ihrem Netzwerk nicht mit Ping überprüfen. Und es wäre fatal, die Firewalls auf allen Computern in Ihrem Subnetz zu deaktivieren. Stattdessen sollten Sie Regeln hinzufügen, die ICMPv4- und ICMPv6-Pakete durch Ihre Firewall erlauben.

Um ICMPv4 zuzulassen, sodass Sie andere Computer mit Ping anhand ihrer IPv4-Adressen testen können, geben Sie auf allen Computern in Ihrem Netzwerk in einer Eingabeaufforderung mit erhöhten Rechten den folgenden Befehl ein:

```
netsh advfirewall firewall add rule name="ICMPv4" protocol=icmpv4:any,any dir=in
action=allow
```

Ähnlich gehen Sie vor, um ICMPv6 zu erlauben, sodass Sie andere Computer anhand ihrer IPv6-Adressen überprüfen können. Geben Sie dazu auf allen Computern in Ihrem Netzwerk in einer Eingabeaufforderung mit erhöhten Rechten den folgenden Befehl ein:

```
netsh advfirewall firewall add rule name="ICMPv6" protocol=icmpv6:any,any dir=in
action=allow
```

Schnelltest

- Wie stellen Sie die Standardeinstellungen der Firewall wieder her?

Antwort zum Schnelltest

- Klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows-Firewall*. Klicken Sie im linken Fensterabschnitt auf *Standard wiederherstellen*.



Prüfungstipp

Denken Sie daran, dass Sie in Windows 7 andere Computer in Ihrem Netzwerk standardmäßig nicht mit Ping überprüfen können.

Abrufen von Netzwerkstatistiken

Wenn Sie Leistungsprobleme untersuchen, die Verbindungen aber prinzipiell funktionieren, brauchen Sie Informationen über die verschiedenen Protokolle, mit denen die Netzwerkkonnektivität implementiert wird. Das Befehlszeilentool *Netstat* zeigt aktive Verbindungen, die vom Computer überwachten Ports, Ethernetstatistiken, die IP-Routingtabelle und IPv4- sowie IPv6-Statistiken an. Wenn Sie das Tool ohne Argumente aufrufen, zeigt es die aktiven Verbindungen an (Abbildung 6.13).

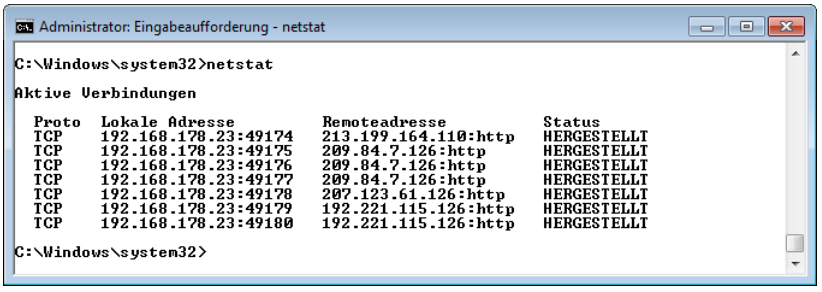


Abbildung 6.13 Der Befehl `netstat` zeigt die aktiven Verbindungen an

Die Syntax des Befehls `netstat` sieht folgendermaßen aus:

`netstat [-a] [-e] [-n] [-o] [-p <Protokoll>] [-r] [-s] [<Intervall>]`

Die Argumente haben folgende Bedeutung:

- **-a** Zeigt alle aktiven Verbindungen sowie die vom Computer überwachten TCP- (Transmission Control Protocol) und UDP-Ports (User Datagram Protocol) an.
- **-e** Zeigt Ethernetstatistiken an, darunter die Zahl der gesendeten und empfangenen Bytes und Pakete. Dieses Argument kann mit `-s` kombiniert werden.
- **-n** Zeigt die aktiven Verbindungen an. Adressen und Portnummern werden numerisch aufgelistet, es wird nicht versucht, die entsprechenden Namen zu ermitteln.
- **-o** Zeigt die aktiven Verbindungen an und gibt zu jeder die Prozess-ID (PID) an. Welche Anwendung zu einer PID gehört, erfahren Sie auf der Registerkarte *Prozesse* im Task-Manager. Dieses Argument kann mit `-a`, `-n` und `-p` kombiniert werden.
- **-p <*Protokoll*>** Zeigt Verbindungen zu dem Protokoll an, das im Parameter *<Protokoll>* angegeben ist. Mögliche Werte sind `tcp`, `udp`, `tcpv6` und `udpv6`. Sie können dieses Argument mit `-s` kombinieren, um Statistiken nach Protokollen aufzugliedern; in diesem Fall sind `tcp`, `udp`, `icmp`, `ip`, `tcpv6`, `udpv6`, `icmpv6` oder `ipv6` möglich.
- **-s** Zeigt Statistiken nach Protokollen aufgegliedert an. In der Standardeinstellung werden Statistiken für die Protokolle TCP, UDP, ICMPv4, ICMPv6, IPv4 und IPv6 ausgegeben. Mit dem Argument `-p` können Sie einen bestimmten Satz Protokolle auswählen.
- **-r** Zeigt den Inhalt der IP-Routingtabelle an. Liefert dieselben Informationen wie der Befehl `route print`.
- ***<Intervall>*** Gibt die ausgewählten Informationen in regelmäßigen Abständen aus. Der Parameter *<Intervall>* legt dabei fest, wie viele Sekunden zwischen jeder Anzeige gewartet wird. Wenn Sie dieses Argument weglassen, gibt Netstat die ausgewählten Informationen nur einmal aus.

Netstat liefert Statistiken zu folgenden Elementen:

- Name des Protokolls (TCP oder UDP)
- IP-Adresse des lokalen Computers und benutzte Portnummer
- IP-Adresse und Portnummer des Remotecomputers
- Status einer TCP-Verbindung



Weitere Informationen Status einer TCP-Verbindung

Weitere Informationen über den Status einer TCP-Verbindung finden Sie unter *http://support.microsoft.com/kb/137984*. Dieser Artikel ist schon älter, die Informationen gelten aber auch noch für Windows 7.

Zum Beispiel zeigt der folgende Befehl sowohl die Ethernetstatistiken als auch die Statistiken zu allen Protokollen an:

```
netstat -e -s
```

Um die TCP-Statistiken für IPv4 zu erhalten, geben Sie diesen Befehl ein:

```
netstat -s -p tcp
```

Abbildung 6.14 zeigt die TCP-Statistiken für das Protokoll IPv4 auf dem Computer *Canberra*.

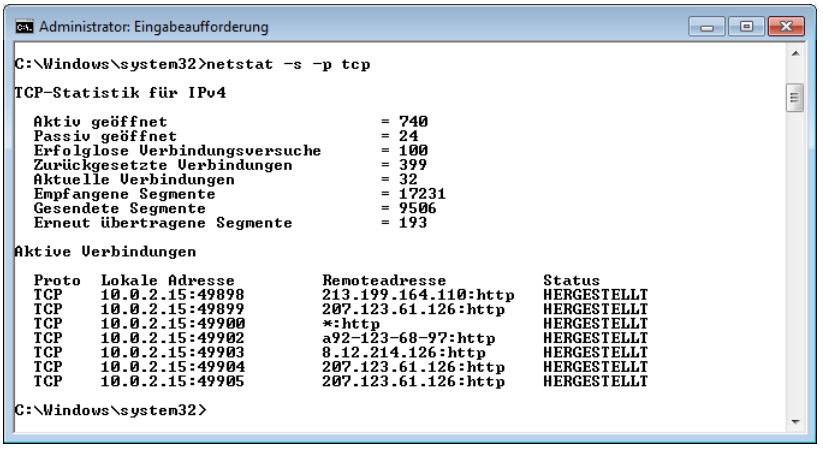


Abbildung 6.14 Statistiken zum Protokoll TCP für IPv4

Übung Konfigurieren von IPv4-Netzwerkverbindungen und Einrichten von ICS

In dieser Übung konfigurieren Sie die Computer *Canberra* und *Aberdeen* mit statischen IPv4-Adressen, konfigurieren die Firewalls auf beiden Computern so, dass sie Ping-Nachrichten erlauben, und testen die Verbindung. Dann ändern Sie die Konfiguration der Computer so, dass sie ihre IPv4-Konfiguration automatisch abrufen, und richten auf *Canberra* ICS so ein, dass beide Computer über die Drahtlosverbindung von *Canberra* auf das Internet zugreifen können.

Übung 1 Konfigurieren der IPv4-Konnektivität

Diese Übung setzt voraus, dass *Canberra* und *Aberdeen* so konfiguriert sind, dass sie ihre IPv4-Konfigurationen automatisch abrufen (Standardeinstellung). Wenn Sie zwei physische Computer verwenden, müssen Sie die beiden an dasselbe Ethernetnetzwerk anschließen, entweder über einen Switch oder Hub oder mit einem Crossover-Ethernetkabel. Gehen Sie folgendermaßen vor, um die IPv4-Konnektivität zu konfigurieren:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
3. Erlauben Sie ICMPv4-Verkehr durch die Firewall von *Canberra*, indem Sie den Befehl **netsh advfirewall firewall add rule name="ICMPv4" protocol=icmpv4:any, any dir=in action=allow** ausführen.
4. Richten Sie eine statische IPv4-Konfiguration ein, indem Sie **netsh interface ipv4 set address "LAN-Verbindung" static 10.0.0.11 255.255.255.0 10.0.0.1** eingeben. Momentan gibt es keinen DNS-Dienst in Ihrem privaten Netzwerk, daher wäre es sinnlos, eine DNS-Einstellung zu konfigurieren. Wenn Sie virtuelle Computer verwenden, hat die Verbindung zu Ihrem privaten Kabelnetzwerk unter Umständen einen anderen Namen als *LAN-Verbindung*.
5. Geben Sie **ipconfig** ein. Ihr Bildschirm müsste nun ähnlich wie in Abbildung 6.15 aussehen.

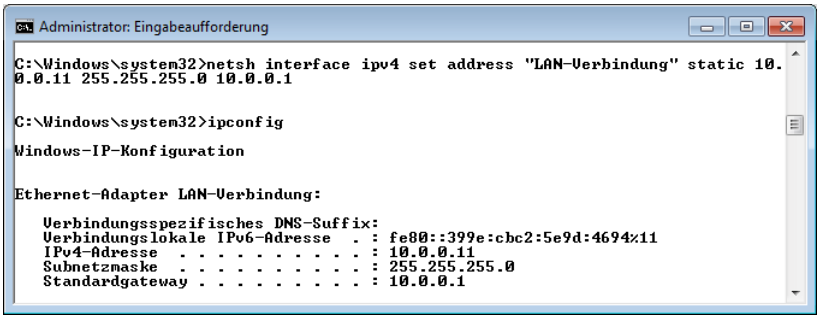

Administrator: Eingabeaufforderung
C:\Windows\system32>netsh interface ipv4 set address "LAN-Verbindung" static 10.0.0.11 255.255.255.0 10.0.0.1
C:\Windows\system32>ipconfig
Windows-IP-Konfiguration
Ethernet-Adapter LAN-Verbindung:
Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse . : fe80::399e:cbc2:5e9d:4694%11
IPv4-Adresse . . . . . : 10.0.0.11
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 10.0.0.1

Abbildung 6.15 Statische Konfiguration des Computers *Canberra*

6. Bleiben Sie auf dem Computer *Canberra* angemeldet. Melden Sie sich auch auf dem Computer *Aberdeen* unter dem Konto *Kim_Akers* an.
7. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
8. Erlauben Sie ICMPv4-Verkehr durch die Firewall von *Aberdeen*, indem Sie den Befehl **netsh advfirewall Firewall add Regelname="ICMPv4" Protokoll=icmpv4:any,any dir=in Aktion=allow** ausführen.
9. Öffnen Sie das Netzwerk- und Freigabecenter. Klicken Sie auf *Adaptereinstellungen ändern*.
10. Klicken Sie mit der rechten Maustaste auf den Ethernet-Adapter *LAN-Verbindung* und wählen Sie den Befehl *Eigenschaften*.
11. Klicken Sie auf *Internetprotokoll Version 4 (TCP/IPv4)* und dann auf die Schaltfläche *Eigenschaften*.
12. Konfigurieren Sie die Verbindung, wie in Abbildung 6.16 gezeigt.
13. Klicken Sie auf *OK* und dann auf *Schließen*.
14. Geben Sie in einer Eingabeaufforderung mit erhöhten Rechten den Befehl **ipconfig** ein. Ihr Bildschirm müsste nun ähnlich wie in Abbildung 6.17 aussehen.
15. Geben Sie **ping 10.0.0.11** ein. Ihr Bildschirm müsste nun ähnlich wie in Abbildung 6.18 aussehen.

16. Geben Sie auf dem Computer *Canberra* den Befehl **ping 10.0.0.21** ein. Prüfen Sie, ob in beiden Richtungen eine Verbindung besteht.
17. Stellen Sie die dynamische IPv4-Konfiguration auf den Computern *Canberra* und *Aberdeen* wieder her.

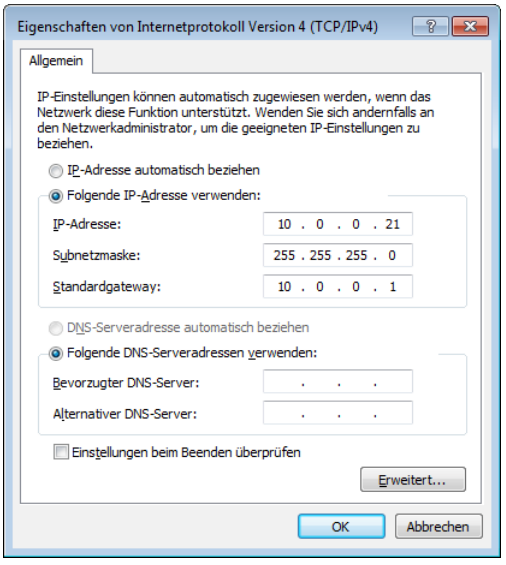

Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 10 . 0 . 0 . 21
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 10 . 0 . 0 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Einstellungen beim Beenden überprüfen
Erweitert...
OK
Abbrechen

Abbildung 6.16 Konfigurieren des Computers *Aberdeen*

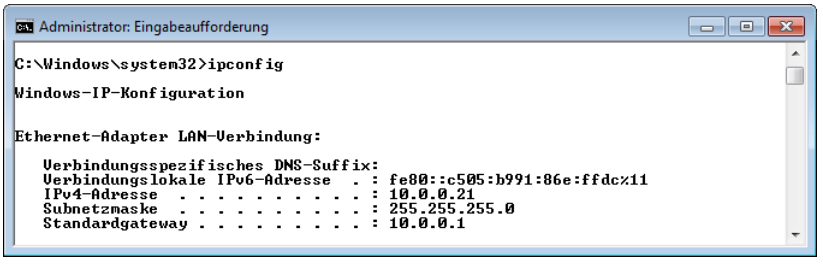

Administrator: Eingabeaufforderung
C:\Windows\system32>ipconfig
Windows-IP-Konfiguration
Ethernet-Adapter LAN-Verbindung:
Verbindungsspezifisches DNS-Suffix:
Verbindungslokale IPv6-Adresse . : fe80::c505:b991:86e:ffdc%11
IPv4-Adresse . . . . . : 10.0.0.21
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : 10.0.0.1

Abbildung 6.17 Statische Konfiguration des Computers *Aberdeen*

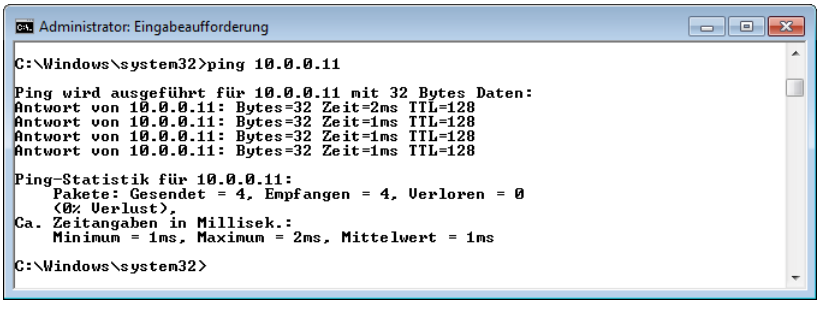

Administrator: Eingabeaufforderung
C:\Windows\system32>ping 10.0.0.11
Ping wird ausgeführt für 10.0.0.11 mit 32 Bytes Daten:
Antwort von 10.0.0.11: Bytes=32 Zeit=2ms TTL=128
Antwort von 10.0.0.11: Bytes=32 Zeit=1ms TTL=128
Antwort von 10.0.0.11: Bytes=32 Zeit=1ms TTL=128
Antwort von 10.0.0.11: Bytes=32 Zeit=1ms TTL=128
Ping-Statistik für 10.0.0.11:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 1ms, Maximum = 2ms, Mittelwert = 1ms
C:\Windows\system32>

Abbildung 6.18 Ping-Test vom Computer *Aberdeen* zum Computer *Canberra*

Übung 2 Konfigurieren von ICS auf dem Computer *Canberra*

In dieser Übung installieren Sie ICS auf dem Computer *Canberra*. Das ermöglicht den Internetzugriff auf *Aberdeen* und stellt sicher, dass *Canberra* DNS- und DHCP-Dienste im Netzwerk bereitstellt. Die Übung setzt voraus, dass *Canberra* über eine Drahtlosverbindung auf das Internet zugreifen kann, daher ist sie optional. Falls auch der Computer *Aberdeen* einen Drahtlosadapter hat, müssen Sie sicherstellen, dass er deaktiviert ist. Stellen Sie außerdem sicher, dass sowohl *Aberdeen* als auch *Canberra* so konfiguriert sind, dass die ihre IPv4-Einstellungen automatisch beziehen.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Öffnen Sie das Netzwerk- und Freigabecenter. Klicken Sie auf *Adaptereinstellungen ändern*.
3. Klicken Sie mit der rechten Maustaste auf den Drahtlosadapter *Drahtlosnetzwerkverbindung* und wählen Sie den Befehl *Eigenschaften*.
4. Klicken Sie auf die Registerkarte *Freigabe*.
5. Aktivieren Sie das Kontrollkästchen *Anderen Benutzern im Netzwerk gestatten, diese Verbindung des Computers als Internetverbindung zu verwenden* (Abbildung 6.19). Klicken Sie auf *OK*.

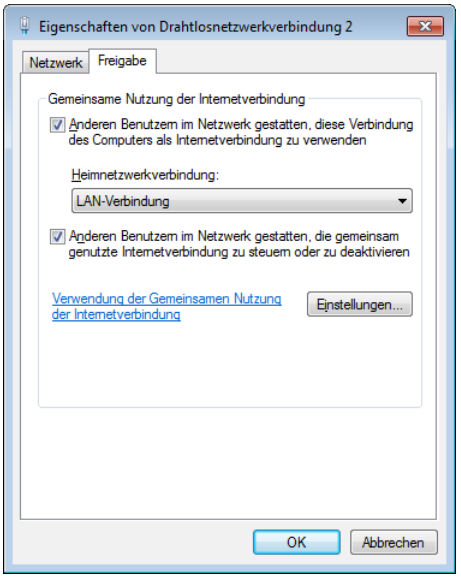

Eigenschaften von Drahtlosnetzwerkverbindung 2
Netzwerk
Freigabe
Gemeinsame Nutzung der Internetverbindung
Anderen Benutzern im Netzwerk gestatten, diese Verbindung des Computers als Internetverbindung zu verwenden
Heimnetzwerkverbindung:
LAN-Verbindung
Anderen Benutzern im Netzwerk gestatten, die gemeinsam genutzte Internetverbindung zu steuern oder zu deaktivieren
Verwendung der Gemeinsamen Nutzung der Internetverbindung
Einstellungen...
OK
Abbrechen

Abbildung 6.19 Andere Computer dürfen die Internetverbindung von *Canberra* benutzen

6. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Aberdeen* an, sofern noch nicht geschehen.
7. Öffnen Sie das Netzwerk- und Freigabecenter. Klicken Sie auf *Internetoptionen*.
8. Klicken Sie auf die Registerkarte *Verbindungen* und stellen Sie sicher, dass die Option *Keine Verbindung wählen* ausgewählt ist.

9. Klicken Sie auf *LAN-Einstellungen*.
10. Deaktivieren Sie im Dialogfeld *Einstellungen für lokales Netzwerk* im Abschnitt *Automatische Konfiguration* die Kontrollkästchen *Automatische Suche der Einstellungen* und *Automatisches Konfigurationsskript verwenden*.
11. Deaktivieren Sie unter *Proxyserver* das Kontrollkästchen *Proxyserver für LAN verwenden*. Das Dialogfeld *Einstellungen für lokales Netzwerk* müsste nun ähnlich wie in Abbildung 6.20 aussehen. Klicken Sie auf *OK*.
12. Klicken Sie auf *OK*, um das Dialogfeld *Eigenschaften von Internet* zu schließen.
13. Öffnen Sie den Windows Internet-Explorer. Sie müssten nun eine Internetverbindung haben. Führen Sie andernfalls die Windows-Netzwerkdiagnose aus.
14. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Geben Sie **ping canberra** ein. Nun steht ein DNS-Dienst zur Verfügung, daher können Sie Computernamen in IPv4-Adressen auflösen.

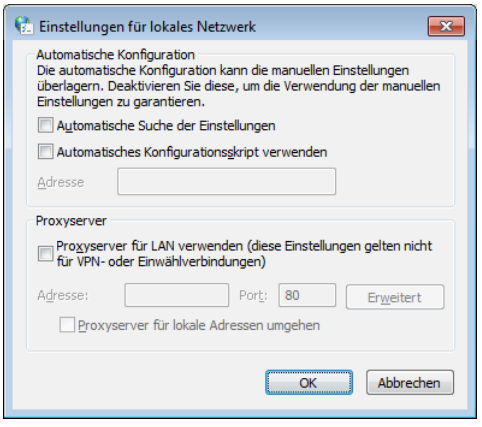


Abbildung 6.20 Das Dialogfeld *Einstellungen für lokales Netzwerk* auf einem ICS-Clientcomputer

Zusammenfassung der Lektion

- IPv4 stellt sicher, dass ein Paket, das über ein IPv4-Netzwerk gesendet wird, sein Ziel erreicht. DHCP konfiguriert Computer in einem Netzwerk automatisch mit IPv4-Einstellungen. DNS löst einen Hostnamen oder FQDN in eine IP-Adresse auf.
- Eine IPv4-Adresse identifiziert einen Computer (oder ein anderes Netzwerkgerät) in einem Subnetz. Eine Subnetzmaske definiert den Bereich der verfügbaren IP-Adressen in einem Subnetz.
- Ein kleineres Kabelnetzwerk, das mehrere Computer enthält, implementiert die TCP/IP-Konfiguration (Transmission Control Protocol/Internet Protocol) üblicherweise mithilfe von ICS. Computer und andere Geräte in einem kleinen Drahtlos- oder Hybridnetzwerk erhalten ihre Konfigurationen meist vom WAP.
- Im Netzwerk- und Freigabecenter können Sie sich die Computer und Geräte in einem Netzwerk ansehen, eine Verbindung zu einem Netzwerk herstellen, eine Verbindung oder ein Netzwerk einrichten und Netzwerkverbindungen verwalten. Sie können auch den Befehl `netsh interface ipv4` verwenden, um IPv4-Netzwerke zu verwalten.

- Sie können die Windows-Netzwerkdiagnose im Netzwerk- und Freigabecenter starten, um Probleme mit einer Netzwerkverbindung zu untersuchen. Kann keine Verbindung zu einer Website hergestellt werden, können Sie dasselbe Tool öffnen, indem Sie auf *Diagnose von Verbindungsproblemen* klicken.
- Mit den Tools Ping, Tracert und Pathping können Sie Probleme mit Netzwerkverbindungen untersuchen. Der Befehl `netstat` gibt Netzwerkprotokollstatistiken aus.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Konfigurieren von IPv4«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welches Befehlszeilentool zeigt die IP-Konfiguration für die Schnittstellen eines Computers an?
   A. Ping
   B. Tracert
   C. Ipconfig
   D. Netstat
2. Wie können Sie die Eigenschaften einer LAN-Verbindung anzeigen? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Klicken Sie im Netzwerk- und Freigabecenter auf *Internetoptionen*. Klicken Sie im Dialogfeld *Eigenschaften von Internet* auf der Registerkarte *Verbindungen* auf *LAN-Einstellungen*.
   B. Klicken Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern*. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung und wählen Sie den Befehl *Status*. Klicken Sie im Dialogfeld *Status von LAN-Verbindung* auf *Eigenschaften*.
   C. Klicken Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern*. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung und wählen Sie den Befehl *Eigenschaften*.
   D. Klicken Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern*. Klicken Sie doppelt auf die LAN-Verbindung. Klicken Sie im Dialogfeld *Status von LAN-Verbindung* auf *Eigenschaften*.
3. Sie konfigurieren in einem isolierten privaten Kabelsubnetz statische IPv4-Adressen für die zwei Computer *Perth* und *Brisbane*. *Perth* bekommt die IPv4-Adresse 172.16.10.140 und die Subnetzmaske 255.255.255.0. Brisbane weisen Sie die IPv4-Adresse 172.16.10. 210 und die Subnetzmaske 255.255.255.0 zu. Sie geben auf *Brisbane* den Befehl **ping 172.16.10.140** ein, aber es wird eine Zeitüberschreitung

gemeldet. Dasselbe Ergebnis bekommen Sie, wenn Sie auf *Perth* den Befehl **ping 172.16.0.210** eingeben, um die IPv4-Adresse von *Brisbane* zu erreichen. Wodurch wird dieser Verbindungsfehler wahrscheinlich verursacht?

A. Im Subnetz ist kein DNS-Dienst verfügbar.

B. Die Computer müssen unterschiedliche Subnetzmasken haben.

C. Sie haben kein Standardgateway angegeben.

D. Sie müssen ICMPv4-Verkehr durch die Firewalls beider Computer erlauben.

4. Sie haben das statisch konfigurierte Kabelsubnetz 10.0.10.128/25 eingerichtet. Momentan ist das einzige Gerät in diesem Subnetz ein Router mit der IPv4-Adresse 10.0.10.129. Sie schließen einen Computer an einen Ethernetanschluss des Subnetzes an. Welcher Befehl konfiguriert den Computer richtig für dieses Subnetz?

   A. `netsh interface ipv4 set address "LAN-Verbindung" static 10.0.10.162 255.255.255.0 10.0.10.129`

   B. `netsh interface ipv4 set address "LAN-Verbindung" static 10.0.0.162 255.255.255.128 10.0.10.129`

   C. `netsh interface ipv4 set address name="LAN-Verbindung" dhcp`

   D. `netsh interface ipv4 set address name="LAN-Verbindung" static 10.0.10.16 255.255.255.128 10.0.10.129`

5. Sie wollen den Inhalt der IPv4- und IPv6-Routentabelle untersuchen. Welchen Befehl verwenden Sie? (Wählen Sie alle zutreffenden Antworten aus.)

   A. `netsh interface ipv4 show route`

   B. `tracert -d`

   C. `route print`

   D. `netstat -r`

   E. `netstat -a`

Lektion 2: Konfigurieren von IPv6

Als Netzwerkexperte haben Sie sicherlich schon mit IPv4 gearbeitet. Weniger vertraut sind Sie wahrscheinlich mit der IPv6-Infrastruktur und den unterschiedlichen Arten von IPv6-Adressen. Da IPv6 immer öfter eingesetzt wird, müssen Sie Strategien für den Umstieg von IPv4 auf IPv6 und die IPv4/IPv6-Interoperabilität kennen, insbesondere Teredo-Adressen. Diese Lektion beschreibt, wie Sie die Namensauflösung für Unicast- und Multicastadressen konfigurieren, eine Netzwerkverbindung konfigurieren und Netzwerkstandorte miteinander verbinden. Außerdem beschreibt sie, wie Sie Konnektivitätsprobleme beseitigen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Erkennen der verschiedenen IPv6-Adresstypen und Erklären ihrer Aufgabe
- Beschreiben der Vorteile von IPv6 und wie sie genutzt werden
- Erkennen von IPv6-Adressen, die im IPv4-Internet weitergeleitet werden können
- Implementieren der IPv4/IPv6-Interoperabilität
- Beseitigen von Problemen bei IPv6-Verbindungen

Veranschlagte Zeit für diese Lektion: 55 Minuten

Aufbau von IPv6-Adressen

IPv4- und IPv6-Adressen lassen sich leicht unterscheiden. Eine IPv4-Adresse verwendet 32 Bits, sodass der Adressraum etwas über 4 Milliarden groß ist. Eine IPv6-Adresse umfasst 128 Bits, der Adressraum umfasst 340.282.366.920.938.463.463.374.607.431.768.211.456 oder 2^{128} Adressen – eine fast unvorstellbar große Zahl. Für jeden Quadratmeter Erdoberfläche stehen $6{,}5 \times 2^{23}$ oder 54.525.952 Adressen zur Verfügung. In der Praxis erlaubt der IPv6-Adressraum mehrere Ebenen der Subnetzunterteilung und der Adresszuweisung zwischen dem Internetbackbone und einzelnen Subnetzen innerhalb einer Organisation. Der viel größere Adressraum ermöglicht es Benutzern, jeder Netzwerkkomponente nicht nur eine, sondern gleich mehrere eindeutige IPv6-Adressen zuzuweisen, wobei jede Adresse einem anderen Zweck dient.

IPv6 stellt einige Adresstypen zur Verfügung, die den IPv4-Adresstypen entsprechen, und weitere, die es nur in IPv6 gibt. Ein Knoten kann mehrere IPv6-Adressen haben, die jeweils andere Aufgaben erfüllen. Dieser Abschnitt beschreibt die Syntax von IPv6-Adressen und die verschiedenen Klassen von IPv6-Adressen.

Syntax einer IPv6-Adresse

Die 128 Bit lange IPv6-Adresse wird in Blöcke von jeweils 16 Bit Länge unterteilt, und jeder 16-Bit-Block wird in eine vierstellige Hexadezimalzahl konvertiert. Doppelpunkte dienen als Trennzeichen zwischen diesen Blöcken. Diese Darstellung wird als *Doppelpunkt-Hexadezimal-Format* bezeichnet.

Globale Unicast-IPv6-Adressen entsprechen den öffentlichen Unicastadressen in IPv4. Sehen wir uns die Syntax von IPv6-Adressen am Beispiel einer globalen IPv6-Unicastadresse an:

21cd:0053:0000:0000:03ad:003f:af37:8d62

Die IPv6-Darstellung kann vereinfacht werden, indem die führenden Nullen in jedem 16-Bit-Block weggelassen werden. Jeder Block muss allerdings mindestens eine Ziffer enthalten. Streichen wir die führenden Nullen, sieht die Adresse so aus:

21cd:53:0:0:3ad:3f:af37:8d62

Eine ununterbrochene Folge von 16-Bit-Blöcken, die den Wert 0 haben, kann im Doppelpunkt-Hexadezimal-Format durch zwei Doppelpunkte (»::«) zusammengefasst werden. Die Beispieladresse lässt sich also auch so schreiben:

21cd:53::3ad:3f:af37:8d62



Hinweis Abgekürzte Schreibweise in IPv6

Sie können in derselben Adresse »::« nicht zweimal verwenden.

Manche Adresstypen enthalten lange Folgen von Nullen, daher lassen sie sich in dieser Notation kompakt darstellen. Zum Beispiel verkürzt sich die Multicastadresse ff05:0:0:0:0:0:0:2 auf ff05::2.

Präfixe von IPv6-Adressen

Das Präfix ist der Teil der Adresse, der angibt, wie viele Bits feste Werte haben, also die Netzwerk-ID enthalten. IPv6-Präfixe werden genauso wie die CIDR-IPv4-Notation in *Schrägstrichnotation* angegeben. Zum Beispiel ist 21cd:53::/64 das Subnetz, in dem die Adresse 21cd:53::23ad:3f:af37:8d62 liegt. In diesem Fall sind die vorderen 64 Bits der Adresse das Netzwerkpräfix. Ein IPv6-Subnetzpräfix (die Subnetz-ID) wird einer einzelnen Verbindung (link) zugewiesen. Derselben Verbindung können mehrere Subnetz-IDs zugewiesen sein. Diese Technik wird als *Multinetting* bezeichnet.



Hinweis IPv6 verwendet in Subnetzmasken keine Punkt-Dezimal-Notation

In IPv6 wird nur die Präfixlängennotation unterstützt. Für die Punkt-Dezimal-Darstellung von IPv4-Subnetzmasken (zum Beispiel 255.255.255.0) gibt es keine direkte Entsprechung.

IPv6-Adresstypen

Es gibt in IPv6 drei Adresstypen:

- **Unicast** Identifiziert eine einzelne Schnittstelle innerhalb des Bereichs des Unicastadresstyps. Pakete, die an eine Unicastadresse gerichtet sind, werden an eine einzige Schnittstelle geliefert. RFC 2373 erlaubt es mehreren Schnittstellen, dieselbe Adresse zu verwenden, sofern diese Schnittstellen für die IPv6-Implementierung auf dem Host wie eine einzige Schnittstelle aussehen. Das ermöglicht Lastverteilungssysteme.
- **Multicast** Identifiziert mehrere Schnittstellen. Pakete, die an eine Multicastadresse gerichtet sind, werden an alle Schnittstellen geliefert, die mit dieser Adresse identifiziert werden.
- **Anycast** Identifiziert mehrere Schnittstellen. Pakete, die an eine Anycastadresse gerichtet sind, werden an die nächstgelegene Schnittstelle geliefert, die durch die Adresse identifiziert wird. Die nächstgelegene Schnittstelle ist die mit der geringsten Routingentfernung oder der geringsten Zahl von Abschnitten (hop). Eine Anycastadresse wird für die Kommunikation von einer Schnittstelle zu einer von mehreren möglichen

Schnittstellen eingesetzt, wobei das Paket letztlich aber nur an eine einzige Schnittstelle geliefert wird.



Weitere Informationen Architektur der IPv6-Adressierung

Weitere Informationen über Struktur und Aufbau von IPv6-Adressen finden Sie unter *http://www.ietf.org/rfc/rfc2373.txt*.



Hinweis Schnittstellen und Knoten

IPv6-Adressen identifizieren Schnittstellen (interface), keine Knoten (node). Ein Knoten wird durch eine Unicastadresse identifiziert, die einer seiner Schnittstellen zugewiesen ist.

IPv6-Unicastadressen

IPv6 unterstützt folgende Typen von Unicastadressen:

- Global
- Verbindungslokal
- Standortlokal
- Speziell

Globale Unicastadressen

Globale Unicastadressen sind das IPv6-Gegenstück zu öffentlichen IPv4-Adressen. Sie sind global routingfähig und im IPv6-Internet erreichbar. Diese Adressen können zusammengefasst werden, um eine effiziente Routinginfrastruktur aufzubauen. Daher werden sie manchmal auch als zusammenfassbare globale Unicastadressen bezeichnet (aggregatable global unicast address). Eine zusammenfassbare globale Unicastadresse ist im gesamten IPv6-Internet eindeutig. (Der Bereich, in dem eine IP-Adresse eindeutig ist, wird als *Gültigkeitsbereich* oder engl. scope bezeichnet.)

Das Formatpräfix (Format Prefix, FP) einer globalen Unicastadresse befindet sich in den drei höchstwertigen Bits, die immer 001 sind. Anders ausgedrückt: Theoretisch können Unicastadressen mit 2 oder 3 beginnen – in der Praxis aber beginnen sie immer mit 2. Eine Beschreibung der internen Struktur einer solchen Adresse würde den Rahmen der Prüfung 70-680 und dieses Buchs sprengen, aber Sie sollten wissen, dass der Abschnitt der Adresse, der den Host definiert (die letzten 64 Bits), entweder von der 48 Bit langen MAC-Hardwareadresse (Media Access Control) der Netzwerkkarte abgeleitet oder der Netzwerkkarte direkt zugewiesen wird. Vereinfacht gesagt, wird die Schnittstellenidentität durch die Netzwerkkartenhardware zur Verfügung gestellt.



Weitere Informationen Aufbau einer globalen Unicastadresse

Weitere Informationen über den Aufbau von globalen Unicastadressen finden Sie in RFC 2374 unter *http://www.ietf.org/rfc/rfc2374.txt*.

Verbindungslokale Adressen

Verbindungslokale (link-local) IPv6-Adressen sind das Gegenstück zu IPv4-Adressen, die über APIPA automatisch konfiguriert werden. Sie erkennen eine verbindungslokale Adresse am FP 1111 1110 10, auf das 54 Nullen folgen. (Verbindungslokale Adressen beginnen also immer mit fe8.) Knoten verwenden verbindungslokale Adressen, wenn sie mit benachbarten Knoten auf derselben Verbindung kommunizieren. Der Gültigkeitsbereich einer verbindungslokalen Adresse ist die lokale Verbindung. Eine verbindungslokale Adresse wird immer automatisch konfiguriert, sogar wenn keine andere Unicastadresse zugewiesen ist.

Standortlokale Adressen

Standortlokale (site-local) IPv6-Adressen sind das Gegenstück zum privaten Adressraum in IPv4. Private Intranets, die keine direkte, weitergeleitete Verbindung in das IPv6-Internet haben, können standortlokale Adressen verwenden, ohne dass ein Konflikt mit zusammenfassbaren globalen Unicastadressen entsteht. Der Gültigkeitsbereich einer standortlokalen Adresse ist der Standort (oder das Internetzwerk der Organisation). Standortlokale Adressen beginnen mit fec0.

Standortlokale Adressen können mithilfe einer statusbehafteten Adresskonfiguration zugewiesen werden, beispielsweise aus einem DHCPv6-Bereich. Ein Host verwendet die statusbehaftete Adresskonfiguration, wenn er Routerankündigungsnachrichten empfängt, die keine Adresspräfixe enthalten. Auch wenn keine Router in der lokalen Verbindung vorhanden sind, verwendet ein Host eine statusbehaftete Adresskonfiguration.

Standortlokale Adressen können auch über statusfreie Adresskonfiguration konfiguriert werden. Sie basiert auf Routerankündigungsnachrichten, die Präfixe für statusfreie Adressen enthalten. In diesem Fall dürfen Hosts kein Protokoll für die statusbehaftete Adresskonfiguration verwenden.

Stattdessen kann die Adresskonfiguration auch eine Kombination von statusfreier und statusbehafteter Konfiguration verwenden. Dieser Fall tritt auf, wenn Routerankündigungsnachrichten Präfixe für statusfreie Adressen enthalten, aber fordern, dass die Hosts ein Protokoll für statusbehaftete Adresskonfiguration verwenden.

Abbildung 6.21 zeigt eine globale Unicastadresse und eine verbindungslokale Adresse, die mit einem Teredo-Tunnel verknüpft sind. Versuchen Sie selbst herauszufinden, zu welcher Klasse jede Adresse gehört. Teredo wird weiter unten in dieser Lektion beschrieben.

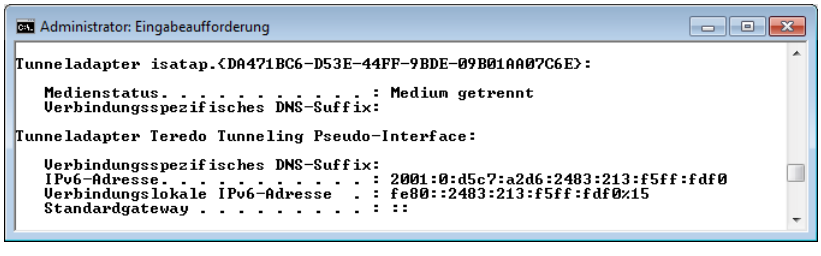

Administrator: Eingabeaufforderung
Tunneladapter isatap.{DA471BC6-D53E-44FF-9BDE-09B01AA07C6E}:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
Tunneladapter Teredo Tunneling Pseudo-Interface:
Verbindungsspezifisches DNS-Suffix:
IPv6-Adresse. . . . . : 2001:0:d5c7:a2d6:2483:213:f5ff:fdf0
Verbindungslokale IPv6-Adresse . : fe80::2483:213:f5ff:fdf0%15
Standardgateway . . . . . : ::

Abbildung 6.21 Eine globale Unicastadresse und eine verbindungslokale Adresse

Verbindungslokale und standortlokale Adressen

Sie können IPv6-Konnektivität zwischen Hosts in einem isolierten Subnetz mithilfe von verbindungslokalen Adressen implementieren. Es ist aber nicht möglich, Routerschnittstellen (Standardgateways) verbindungslokale Adressen zuzuweisen, und es ist kein Routing von einem Subnetz in ein anderes verfügbar, falls nur verbindungslokale Adressen benutzt werden. Bei DNS-Servern ist es nicht möglich, ausschließlich verbindungslokale Adressen zu verwenden. Wenn Sie verbindungslokale Adressen benutzen, müssen Sie ihre Schnittstellen-IDs angeben – das ist die Zahl hinter dem Prozentzeichen am Ende der Adresse. Verbindungslokale Adressen werden in Windows-DDNS nicht dynamisch registriert.

Aus diesen Gründen werden in Subnetzen eines privaten Netzwerks normalerweise standortlokale Adressen benutzt, um IPv6-Konnektivität über das gesamte Netzwerk zu implementieren. Sofern jedes Gerät im Netzwerk eine eigene globale Adresse hat (ein Ziel der IPv6-Implementierung), können Sie globale Adressen verwenden, um das Routing zwischen internen Subnetzen, in periphere Zonen und in das Internet zu ermöglichen.

Spezielle Adressen

Es gibt zwei spezielle IPv6-Adressen: die unspezifizierte Adresse und die Loopbackadresse. Die unspezifizierte Adresse 0:0:0:0:0:0:0:0 (oder ::) steht für das Fehlen einer Adresse, sie ist das Gegenstück zur unspezifizierten IPv4-Adresse 0.0.0.0. Normalerweise wird sie als Quelladresse für Pakete eingetragen, mit denen überprüft wird, ob eine vorläufige Adresse eindeutig ist. Sie wird niemals einer Schnittstelle zugewiesen oder als Zieladresse verwendet. Die Loopbackadresse 0:0:0:0:0:0:0:1 (oder ::1) identifiziert eine Loopbackschnittstelle, sie ist das Gegenstück zur IPv4-Loopbackadresse 127.0.0.1.

IPv6-Multicastadressen

Mithilfe einer IPv6-Multicastadresse kann ein IPv6-Paket an mehrere Hosts gesendet werden, die alle dieselbe Multicastadresse haben. Das FP lautet 11111111, Multicastadressen beginnen also immer mit ff.

Schnelltest

- Welchen Typ hat die Adresse fec0:0:0:eadf::1ff?

Antwort zum Schnelltest

- Standortlokale Unicastadresse

IPv6-Anycastadressen

Eine Anycastadresse ist mehreren Schnittstellen zugewiesen. Pakete, die an eine Anycastadresse gerichtet sind, werden von der Routinginfrastruktur an die nächstgelegene dieser Schnittstellen weitergeleitet. Der Routinginfrastruktur muss bekannt sein, welchen Schnittstellen Anycastadressen zugewiesen sind und wie weit sie im Bezug auf die Routingmetrik entfernt sind. Momentan werden Anycastadressen nur als Zieladressen verwendet, und sie werden nur Routern zugewiesen.



Prüfungstipp

Eine globale Unicastadresse ist das IPv6-Gegenstück zu einer öffentlichen Unicastadresse in IPv4. Normalerweise beginnt sie mit einer 2. Eine verbindungslokale IPv6-Adresse ist das Gegenstück zu einer APIPA-Adresse in IPv4, sie beginnt mit fe8. Eine standortlokale IPv6-Adresse ist das Gegenstück zu einer privaten IPv4-Adresse, sie beginnt mit fec0. Die speziellen IPv6-Adressen :: und ::1 sind die Gegenstücke zu den IPv4-Adressen 0.0.0.0 und 127.0.0.1. IPv6-Multicastadressen beginnen mit ff. Anycastadressen werden nur Routern zugewiesen, sie werden in der Prüfung 70-680 nicht behandelt.

Die Vorteile von IPv6

IPv6 wurde entworfen, um die Einschränkungen von IPv4 zu überwinden. Gegenüber seinem Vorgänger hat IPv6 zahlreiche Vorteile:

- **Größerer Adressraum** IPv6 stellt genug Adressen für jedes Gerät zur Verfügung, das eine eindeutige öffentliche IPv6-Adresse braucht. Außerdem kann der 64-Bit-Hostabschnitt (Schnittstellen-ID) einer IPv6-Adresse automatisch aus der Netzwerkkartenhardware generiert werden.
- **Automatische Adresskonfiguration** IPv4 wird normalerweise von Hand oder mithilfe von DHCP konfiguriert. Die automatische Konfiguration (Autokonfiguration) mit APIPA ist nur in isolierten Subnetzen möglich, deren Verkehr nicht in andere Netzwerke weitergeleitet wird. IPv6 bietet eine einfache, automatische Adresskonfiguration, indem es sowohl statusbehaftete als auch statusfreie Adresskonfiguration unterstützt.
- **Sicherheit auf Netzwerkebene** Bei der Kommunikation über das Internet ist Verschlüsselung nötig, um zu verhindern, dass Daten unterwegs ausgespäht oder manipuliert werden. IPSec (Internet Protocol Security) bietet diese Möglichkeit, und IPv6 macht IPSec obligatorisch.
- **Datenauslieferung in Echtzeit** In IPv4 gibt es Quality of Service (QoS), und für Echtzeitverkehr über ein Netzwerk kann Bandbreite garantiert werden. Das gilt aber nicht, wenn die Nutzdaten eines IPv4-Pakets verschlüsselt sind. Im Feld `Flow Label` des IPv6-Headers ist eine Nutzdatenidentifizierung eingebaut, sodass der QoS-Betrieb nicht durch die Verschlüsselung der Nutzdaten beeinträchtigt wird.
- **Größe der Routingtabelle** Im IPv6-Internet sind die Routingtabellen von Backboneroutern dank Routenzusammenfassung deutlich kleiner, weil mehrere aneinandergrenzende Adressblöcke kombiniert und als größerer Adressblock zusammengefasst werden können.
- **Headergröße und Erweiterungsheader** IPv4- und IPv6-Header sind nicht kompatibel, und ein Host oder Router muss IPv4- und IPv6-Implementierungen enthalten, um beide Headerformate zu erkennen und zu verarbeiten. Daher wurde der IPv6-Header möglichst kompakt aufgebaut. Alle nicht unbedingt benötigten und optionalen Felder wurden in Erweiterungsheader verschoben, die auf den IPv6-Header folgen.
- **Kein Broadcastverkehr mehr** IPv4 nutzt ARP-Broadcasts, um die MAC-Adressen der Netzwerkkarten aufzulösen. Das IPv6-Nachbarermittlungsprotokoll (Neighbor Discovery, ND) arbeitet mit einer Abfolge von ICMPv6-Nachrichten. ND ersetzt ARP-Broadcasts, ICMPv4-Routersuche und ICMPv4-Umleitungsnachrichten durch effiziente Multicast- und Unicast-ND-Nachrichten.

Schnelltest

1. Wie Viele Bits umfasst eine IPv4-Adresse?
2. Wie viele Bits umfasst eine IPv6-Adresse?

Antworten zum Schnelltest

1. 32
2. 128

Adressenauflösung in IPv6

Das ND-Protokoll löst IPv6-Adressen in MAC-Adressen auf. Das ist in den meisten Fällen ein simpler Vorgang. Beispielsweise leitet sich der 64 Bit lange Hostabschnitt einer globalen IPv6-Unicastadresse aus der MAC-Adresse der Netzwerkkarte ab.

Die Auflösung von Hostnamen in IPv6-Adressen wird mithilfe von DNS durchgeführt (außer bei verbindungslokalen Adressen, die nicht in DNS gespeichert, sondern automatisch aufgelöst werden). Der Ablauf ist derselbe wie bei der IPv4-Adressenauflösung. Das Wertepaar aus Computername und IPv6-Adresse wird in einem AAAA-DNS-Ressourceneintrag gespeichert, dem Gegenstück zum A- oder Hosteintrag bei IPv4. Reverse-DNS-Lookups, die den Computernamen zu einer IPv6-Adresse liefern, sind mit einem PTR-DNS-Ressourceneintrag implementiert, der über die IPv6-Reverse-Lookupzone *ipv6.arpa* führt; dies ist das Gegenstück zur Reverse-Lookupzone *in-addr.arpa* in IPv4.

Eine *ipv6.arpa*-Reverse-Lookupzone zu erstellen, ist ein komplexer Vorgang, bei der die IPv6-Adresse in 4-Bit-Blöcke unterteilt und in umgekehrter Reihenfolge eingegeben wird. Dies würde den Rahmen von Prüfung 70-680 sprengen.

In Peer-to-Peer-Umgebungen, wo kein DNS verfügbar ist (beispielsweise in Ad-hoc-Netzwerken), bietet PNRP (Peer Name Resolution Protocol) dynamische Namenregistrierung und Namensauflösung. PNRP kann Peernamen mit dem Computer oder einzelnen Anwendungen und Diensten des Computers verknüpfen. Eine Peernamensauflösung umfasst eine Adresse, den Port und manchmal erweiterte Nutzdaten. Peernamen können geschützt oder ungeschützt veröffentlicht werden. PNRP benutzt Kryptografie mit öffentlichen Schlüsseln, um geschützte Peernamen vor Spoofing zu schützen.



Weitere Informationen Peer Name Resolution-Protokoll

Weitere Informationen über PNRP finden Sie unter *http://msdn.microsoft.com/en-us/library/bb968779.aspx*.

Implementieren von IPv4-zu-IPv6-Kompatibilität

Neben den verschiedenen Adresstypen, die weiter oben in dieser Lektion beschrieben wurden, stellt IPv6 die folgenden Typen von Kompatibilitätsadressen zur Verfügung, um die Migration von IPv4 auf IPv6 zu unterstützen und Übergangstechnologien zu implementieren.

IPv4-kompatible Adresse

Die IPv4-kompatible Adresse 0:0:0:0:0:0:w.x.y.z (oder ::w.x.y.z) wird von Dual-Stack-Knoten benutzt, die über eine IPv4-Infrastruktur mit IPv6 kommunizieren. Die letzten vier

Oktette (w.x.y.z) stehen für die Punkt-Dezimal-Darstellung einer IPv4-Adresse. Wenn die IPv4-kompatible Adresse als IPv6-Ziel angegeben ist, wird IPv6-Verkehr automatisch mit einem IPv4-Header gekapselt und über die IPv4-Infrastruktur an das Ziel gesendet.

IPv4-zugeordnete Adresse

Die IPv4-zugeordnete Adresse 0:0:0:0:0:ffff:w.x.y.z (oder ::fffff:w.x.y.z) wird benutzt, um einem reinen IPv4-Knoten einen IPv6-Knoten bekannt zu machen und somit IPv4-Geräte, die nicht zu IPv6 kompatibel sind, im IPv6-Adressraum zuzuordnen.

6to4-Adresse

Mithilfe einer 6to4-Adresse können IPv6-Pakete über ein IPv4-Netzwerk (im Allgemeinen das IPv4-Internet) befördert werden, ohne dass explizite Tunnel konfiguriert werden müssen. 6to4-Hosts können mit Hosts im IPv6-Internet kommunizieren. Meist wird eine 6to4-Adresse verwendet, wenn ein Benutzer über eine bereits vorhandene IPv4-Verbindung eine Verbindung zum IPv6-Internet aufbauen will. Diese Adressen haben die Form 2002:<*erstes und zweites Byte der IPv4-Adresse*>:<*drittes und viertes Byte der IPv4-Adresse*>::/16.

Um eine 6to4-Adresse zu benutzen, brauchen Sie IPv6 nicht auf den benachbarten Geräten des Hosts zu konfigurieren oder zu unterstützen. Daher ist 6to4 besonders während der Anfangsphasen bei der Umstellung auf vollständige, native IPv6-Konnektivität wichtig. Es soll ausschließlich als Übergangsmechanismus dienen, keinesfalls als Dauerlösung. Es ermöglicht keine Kommunikation zwischen reinen IPv4- und reinen IPv6-Hosts.

Teredo-Adresse

Eine Teredo-Adresse enthält ein 32-Bit-Teredo-Präfix. In Windows 7 (und Windows Vista sowie Windows Server 2008) lautet es 2001::/32. Auf das Präfix folgt die 32 Bit lange, öffentliche IPv4-Adresse des Teredo-Servers, der bei der Konfiguration der Adresse mitgewirkt hat. Die nächsten 16 Bits sind für Teredo-Flags reserviert. Momentan ist nur das höchstwertige Flagbit definiert. Dies ist das `Cone`-Flag. Es ist gesetzt, wenn das NAT, das mit dem Internet verbunden ist, ein Cone-NAT ist.



Hinweis Teredo in Windows XP und Windows Server 2003

In Windows XP und Windows Server 2003 war das Teredo-Präfix ursprünglich 3ffe:831f::/32. Computer, die unter Windows XP und Windows Server 2003 laufen, verwenden das Teredo-Präfix 2001::/32, wenn sie mit dem Microsoft Security Bulletin MS06-064 aktualisiert wurden.

Die nächsten 16 Bits speichern eine unkenntlich gemachte Version der externen UDP-Portnummer, die den gesamten Teredo-Verkehr für die Teredo-Clientschnittstelle abwickelt. Wenn ein Teredo-Client sein erstes Paket an einen Teredo-Server sendet, ordnet NAT den Quell-UDP-Port des Pakets einem anderen, externen UDP-Port zu. Der gesamte Teredo-Verkehr für die Hostschnittstelle verwendet denselben externen, zugeordneten UDP-Port. Die Nummer dieses externen Ports wird maskiert oder verschleiert, indem eine XOR-Operation mit dem Wert 0xffff durchgeführt wird. Diese Verschleierung des externen Ports verhindert, dass NATs sie innerhalb der Nutzdaten der weitergeleiteten Pakete umsetzen.

Die letzten 32 Bits speichern eine verschleierte Version der externen IPv4-Adresse, die den gesamten Teredo-Verkehr für die Teredo-Clientschnittstelle abwickelt. Die externe Adresse

wird dadurch verschleiert, dass eine XOR-Operation mit 0xffffffff durchgeführt wird. Wie beim UDP-Port verhindert dies, dass NAT-Geräte die externe IPv4-Adresse innerhalb der Nutzdaten von Paketen umsetzen, die weitergeleitet werden.

Die externe Adresse wird dadurch verschleiert, dass sie in einer XOR-Operation mit dem Wert 0xffffffff verknüpft wird. Zum Beispiel lautet die verschleierte Version der öffentlichen IPv4-Adresse 131.107.0.1 im Doppelpunkt-Hexadezimal-Format 7c94:fffe. (131.107.0.1 entspricht 0x836b0001 im Hexadezimalformat, und 0x836b0001 XOR 0xffffffff ergibt 0x7c94fffe.) Das Verschleiern der externen Adresse verhindert, dass NAT-Geräte sie innerhalb der Nutzdaten der Pakete umsetzen, die weitergeleitet werden.

Sehen wir uns ein Beispiel an. Northwind Traders implementiert momentan folgende private IPv4-Netzwerke in seiner Hauptstelle und den Zweigstellen:

- Hauptstelle: 10.0.100.0 /24
- Zweigstelle 1: 10.0.0.0 /24
- Zweigstelle 2: 10.0.10.0 /24
- Zweigstelle 3: 10.0.20.0 /24

Das Unternehmen will IPv6-Kommunikation zwischen mehreren Teredo-Clients sowie zwischen Teredo-Clients und reinen IPv6-Hosts ermöglichen. Weil Teredo-Server im IPv4-Internet vorhanden sind, kann diese Kommunikation implementiert werden. Ein Teredo-Server ist ein IPv6/IPv4-Knoten, der sowohl mit dem IPv4-Internet als auch dem IPv6-Internet verbunden ist und eine Teredo-Tunnelschnittstelle unterstützt. Wie die Teredo-Adressen der Netzwerke von Northwind Traders lauten, hängt von einer Reihe von Faktoren ab, zum Beispiel dem Port und dem Typ des verwendeten NAT-Servers. Sie können beispielsweise folgendermaßen lauten:

- Hauptstelle: 2001::ce49:7601:e866:efff:f5ff:9bfe bis 2001::0a0a:64fe:e866:efff:f5ff:9b01
- Zweigstelle 1: 2001:: ce49:7601:e866:efff:f5ff:fffe bis 2001::0a0a:0afe:e866:efff:f5ff:ff01
- Zweigstelle 2: 2001:: ce49:7601:e866:efff:f5ff:f5fe bis 2001::0a0a:14fe:e866:efff:f5ff:f501
- Zweigstelle 3: 2001:: ce49:7601:e866:efff:f5ff:ebfe bis 2001::0a0a:1efe:e866:efff:f5ff:ebfe

Beachten Sie, dass 10.0.100.1 in diesem Beispiel 0a00:6401 entspricht, und 0a00:6401 XOR ffff:ffff den Wert f5ff:9bfe ergibt.



Prüfungstipp

In den Zielen von Prüfung 70-680 werden die von Microsoft unterstützten Teredo-Adressen explizit erwähnt. Es ist aber unwahrscheinlich, dass Sie in der Prüfung eine Teredo-Adresse generieren müssen. Unter Umständen müssen Sie eine solche Adresse erkennen und die enthaltene IPv4-Adresse extrahieren. Glücklicherweise haben Sie während der Prüfung Zugriff auf einen wissenschaftlichen Taschenrechner. Wahrscheinlicher ist, dass Sie eine Teredo- oder eine 6to4-Adresse identifizieren müssen. Beides sind öffentliche Adressen. Eine Teredo-Adresse beginnt mit 2001, eine 6to4-Adresse mit 2002.



Hinweis Teredo

Weitere Informationen über Teredo finden Sie unter *http://www.ietf.org/rfc/rfc4380.txt* und *http://www.microsoft.com/technet/network/ipv6/teredo.mspx*.

Cone-NATs

Cone-NATs können im Full-Cone-, Restricted-Cone- oder Port-Restricted-Cone-Modus arbeiten. Bei einem Full-Cone-NAT werden alle Anforderungen, die von derselben Kombination aus interner IP-Adresse und Port stammen, derselben Kombination aus externer IP-Adresse und Port zugewiesen, und jeder externe Host kann ein Paket an den internen Host senden, indem er ein Paket an die zugewiesene Adresse schickt.

Bei einem Restricted-Cone-NAT werden alle Anforderungen, die von derselben Kombination aus interner IP-Adresse und Port stammen, derselben Kombination aus externer IP-Adresse und Port zugewiesen, aber ein externer Host kann nur dann ein Paket an den internen Host senden, wenn der interne Host vorher schon ein Paket an den externen Host geschickt hat.

Bei einem Port-Restricted-Cone-NAT werden auch Portnummern eingeschränkt. Ein externer Host mit einer angegebenen Kombination aus IP-Adresse und Quellport kann nur dann ein Paket an einen internen Host senden, wenn der interne Host vorher bereits ein Paket an diese Kombination aus IP-Adresse und Port gesendet hat.

ISATAP-Adressen

IPv6 kann eine ISATAP-Adresse (Intra-Site Automatic Tunneling Addressing Protocol) nutzen, um die Kommunikation zwischen zwei Knoten über ein IPv4-Intranet herzustellen. Eine ISATAP-Adresse beginnt mit einem 64 Bit langen verbindungslokalen, standortlokalen, globalen oder 6to4-globalen Unicastpräfix. Die nächsten 32 Bits sind die ISATAP-Kennung 0:5efe. Die letzten 32 Bits enthalten die IPv4-Adresse in Punkt-Dezimal- oder Hexadezimalnotation. Eine ISATAP-Adresse steht entweder für eine öffentliche oder eine private IPv4-Adresse. Sie erkennen eine ISATAP-Adresse an der Ziffernfolge 5efe, auf die eine IP-Adresse in Punkt-Dezimal- oder Hexadezimalformat folgt.

Implementieren von IPv6-zu-IPv4-Kompatibilität

Sie implementieren die IPv6-zu-IPv4-Kompatibilität mit den Befehlen `netsh interface ipv6 6to4`, `netsh interface ipv6 isatap` oder `netsh interface ipv6 add v6v4tunnel`. So erstellt der folgende Befehl einen IPv6-in-IPv4-Tunnel zwischen der lokalen Adresse 10.0.0.11 und der Remoteadresse 192.168.123.116 auf einer Schnittstelle namens *Remote*: `netsh interface ipv6 add v6v4tunnel "Remote" 10.0.0.11 192.168.123.116`.



Hinweis Übergangstechnologien

Die verschiedenen Methoden, um IPv6-zu-IPv4-Kompatibilität zu implementieren, werden als *Übergangstechnologien* (transition technologies) bezeichnet.



Hinweis 6to4cfg

Windows 7 unterstützt das Tool 6to4cfg nicht.

Konfigurieren von IPv6-Verbindungen

Windows 7 stellt Tools zur Verfügung, mit denen Sie IPv6-Schnittstellen konfigurieren sowie IPv6-Konnektivität und -Routing prüfen können. Außerdem gibt es Tools, die IPv4-zu-IPv6-Kompatibilität aktivieren und prüfen.

In Windows 7 bieten die Standardbefehlszeilentools wie Ping, Ipconfig, Pathping, Tracert, Netstat und Route vollständige IPv6-Unterstützung. Zum Beispiel zeigt Abbildung 6.22, wie mit Ping eine verbindungslokale IPv6-Adresse auf dem Computer *Canberra* geprüft wird. Die IPv6-Adresse in Ihrem Testnetzwerk hat einen anderen Wert. Wenn Sie von einem Host aus die verbindungslokale Adresse eines anderen mit Ping überprüfen wollen, müssen Sie die Schnittstellen-ID mit angeben, zum Beispiel `ping fe80::d1ff:d166:7888:2fd6%12`. Schnittstellen-IDs werden weiter unten in dieser Lektion genauer beschrieben. Beachten Sie, dass dieser Befehl deshalb funktioniert, weil Sie eine verbindungslokale Adresse auf demselben Computer anpingen. Ping-Tests zwischen Computern funktionieren nur, wenn Sie ICMPv6-Verkehr durch die Firewalls aller beteiligten Computer erlauben.

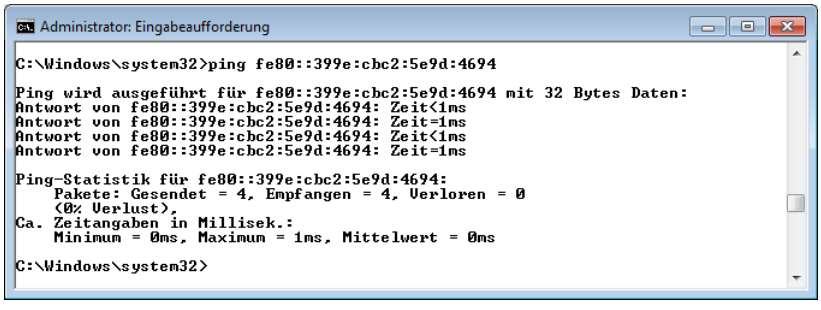

Administrator: Eingabeaufforderung
C:\Windows\system32>ping fe80::399e:cbc2:5e9d:4694
Ping wird ausgeführt für fe80::399e:cbc2:5e9d:4694 mit 32 Bytes Daten:
Antwort von fe80::399e:cbc2:5e9d:4694: Zeit<1ms
Antwort von fe80::399e:cbc2:5e9d:4694: Zeit=1ms
Antwort von fe80::399e:cbc2:5e9d:4694: Zeit<1ms
Antwort von fe80::399e:cbc2:5e9d:4694: Zeit=1ms
Ping-Statistik für fe80::399e:cbc2:5e9d:4694:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms
C:\Windows\system32>

Abbildung 6.22 Ping-Test einer verbindungslokalen IPv6-Adresse



Hinweis PING6

Das Befehlszeilentool Ping6 wird in Windows 7 nicht unterstützt.

Spezielle Tools für IPv6 stellt Netsh bereit. Zum Beispiel zeigt der Befehl `netsh interface ipv6 show neighbors` die IPv6-Schnittstellen aller Hosts im lokalen Subnetz an. Sie verwenden diesen Befehl in den Übungen am Ende dieser Lektion, nachdem Sie die IPv6-Konnektivität in einem Subnetz konfiguriert haben.

Überprüfen von IPv6-Konfiguration und -Konnektivität

Wenn Sie Verbindungsprobleme untersuchen oder einfach Ihre Konfiguration überprüfen wollen, ist das wahrscheinlich nützlichste und am häufigsten benutzte Tool Ipconfig. Der Befehl `ipconfig /all` zeigt sowohl die IPv4- als auch die IPv6-Konfiguration an. Eine Ausgabe dieses Tools sehen Sie in Abbildung 6.6 weiter oben in dieser Lektion.

Wenn Sie nur die Konfiguration der IPv6-Schnittstellen auf dem lokalen Computer anzeigen wollen, können Sie den Befehl `netsh interface ipv6 show address` verwenden. Abbildung 6.23 zeigt die Ausgabe dieses Befehls auf dem Computer *Canberra*. Beachten Sie das Prozentzeichen und die Zahl, die hinter jeder IPv6-Adresse stehen. Dies ist die Schnittstellen-ID. Sie identifiziert die Schnittstelle, die für die IPv6-Adresse konfiguriert ist.

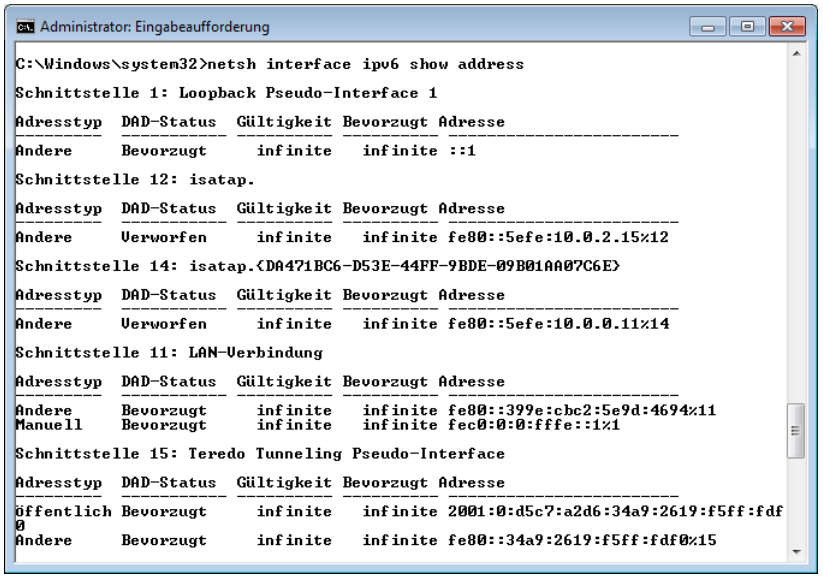

Administrator: Eingabeaufforderung
C:\Windows\system32>netsh interface ipv6 show address
Schnittstelle 1: Loopback Pseudo-Interface 1
Adresstyp DAD-Status Gültigkeit Bevorzugt Adresse
Andere Bevorzugt infinite infinite ::1
Schnittstelle 12: isatap.
Adresstyp DAD-Status Gültigkeit Bevorzugt Adresse
Andere Verworfen infinite infinite fe80::5efe:10.0.2.15%12
Schnittstelle 14: isatap.{DA471BC6-D53E-44FF-9BDE-09B01AA07C6E}
Adresstyp DAD-Status Gültigkeit Bevorzugt Adresse
Andere Verworfen infinite infinite fe80::5efe:10.0.0.11%14
Schnittstelle 11: LAN-Verbindung
Adresstyp DAD-Status Gültigkeit Bevorzugt Adresse
Andere Bevorzugt infinite infinite fe80::399e:cbc2:5e9d:4694%11
Manuell Bevorzugt infinite infinite fec0:0:0:fffe::1%1
Schnittstelle 15: Teredo Tunneling Pseudo-Interface
Adresstyp DAD-Status Gültigkeit Bevorzugt Adresse
öffentlich Bevorzugt infinite infinite 2001:0:d5c7:a2d6:34a9:2619:f5ff:fdf
0
Andere Bevorzugt infinite infinite fe80::34a9:2619:f5ff:fdf0%15

Abbildung 6.23 Anzeigen von IPv6-Adressen und Schnittstellen-IDs



Hinweis **Das Dialogfeld *Netzwerkverbindungsdetails***

Die IPv6-Adresse einer Schnittstelle erfahren Sie auch, wenn Sie das Dialogfeld *Netzwerkverbindungsdetails* öffnen. Wie das geht, wird in Lektion 3 beschrieben, ein Beispiel für das Dialogfeld sehen Sie in Abbildung 6.38 dieser Lektion. Im Dialogfeld *Netzwerkverbindungsdetails* wird allerdings nicht die Schnittstellen-ID angezeigt.

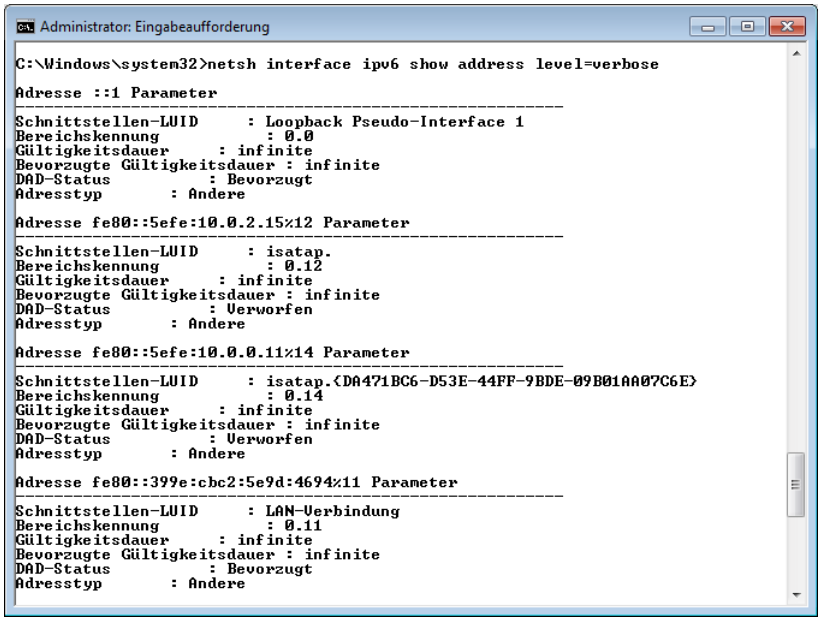


Abbildung 6.24 Anzeigen von IPv6-Adressen und Standort-IDs

Wenn Sie ein großes Unternehmensnetzwerk mit mehreren Standorten administrieren, müssen Sie auch die Standort-IDs wissen. Eine Standort-ID ermitteln Sie mit dem Befehl **netsh interface ipv6 show address level=verbose**. Einen Teil der Ausgabe dieses Befehls zeigt Abbildung 6.24.

Konfigurieren von IPv6-Schnittstellen

Die meisten IPv6-Adressen werden im Normalfall über Autokonfiguration oder DHCPv6 konfiguriert. Wenn Sie eine IPv6-Adresse von Hand konfigurieren wollen, können Sie den Befehl `netsh interface ipv6 set address` verwenden. Hier ein Beispiel: `netsh interface ipv6 set address "LAN-Verbindung 2" fec0:0:0:ffee:2`. Sie müssen die Eingabeaufforderung als Administrator ausführen, wenn Sie diesen Befehl eingeben. In Windows 7 können Sie IPv6-Adressen auch im Dialogfeld *Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6)* von Hand konfigurieren. Abbildung 6.25 zeigt diese Konfiguration.

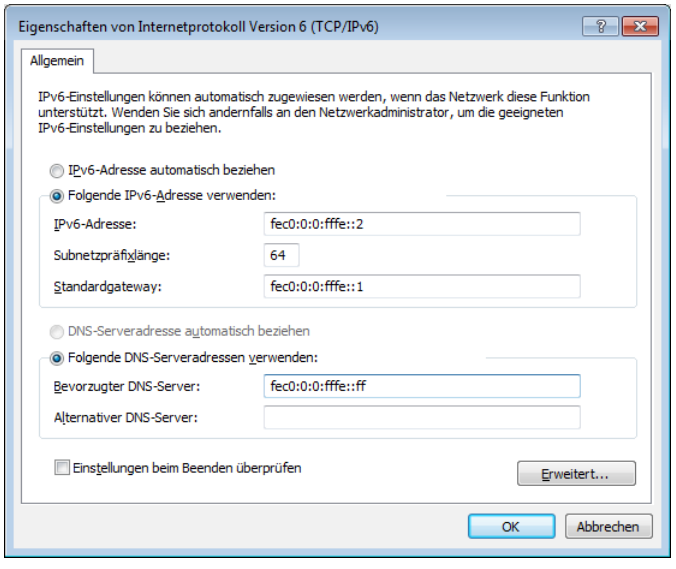


Abbildung 6.25 Konfigurieren einer IPv6-Adresse über einen Windows-Dialog

Der Vorteil bei dieser TCP/IPv6-Bedienungsoberfläche ist, dass Sie neben der Schnittstellenadresse auch gleich die IPv6-Adressen der DNS-Server eingeben können. Wenn Sie dagegen die Befehlszeile verwenden, lautet der Befehl zum Hinzufügen der IPv6-Adressen von DNS-Servern `netsh interface ipv6 add dnsserver`, zum Beispiel **netsh interface ipv6 add dnsserver "LAN-Verbindung" fec0:0:0:ffee::ff**. Der Befehl, um ein Standardgateway hinzuzufügen, lautet `netsh interface ipv6 add route`, gefolgt von der Metrik (der Vorrangreihenfolge für den Fall, dass mehrere Routen zur Verfügung stehen). Hier wiederum ein Beispiel: **netsh interface ipv6 add route ::/0 "LAN-Verbindung" fec0:0:0:ffee::1**.

Die Eigenschaften von IPv6-Schnittstellen (aber nicht ihre Konfiguration) ändern Sie mit dem Befehl `netsh interface ipv6 set interface`, zum Beispiel **netsh interface ipv6 set interface "LAN-Verbindung" forwarding=enabled**. Sie müssen die Eingabeaufforderung als Administrator ausführen, wenn Sie einen der Konfigurationsbefehle von Netsh verwenden.



Weitere Informationen Netsh

Netsh ist ein außergewöhnlich leistungsfähiges und vielseitiges Tool, mit dem Sie sehr viele Konfigurationsaufgaben über eine Befehlszeilenschnittstelle erledigen können. Weitere Informationen finden Sie unter *http://technet.microsoft.com/de-de/library/cc785383.aspx*.

Schnelltest

- Welcher Netsh-Befehl listet die Standort-IDs auf?

Antwort zum Schnelltest

- `netsh interface ipv6 show address level=verbose`

Überprüfen der IPv6-Konnektivität

Wenn Sie die Konnektivität in einem LAN überprüfen, sollten Sie als Erstes den Nachbarcache löschen, der vor Kurzem aufgelöste Verbindungsschichtadressen speichert und möglicherweise ein falsches Ergebnis liefert, falls Sie Änderungen im Bereich der Adressenauflösung vorgenommen haben. Sie prüfen den Inhalt des Nachbarcaches mit dem Befehl `netsh interface ipv6 show neighbors`. Der Befehl `netsh interface ipv6 delete neighbors` leert den Cache. Sie müssen die Eingabeaufforderung als Administrator ausführen, wenn Sie diese Befehle verwenden.

Die Konnektivität zu einem lokalen Host in Ihrem Subnetz und zu Ihrem Standardgateway testen Sie mit dem Tool Ping. Beachten Sie, dass die Windows-Firewall in der Standardeinstellung Ping-Befehle blockiert. Daher müssen Sie ICMPv6-Pakete durch die Firewalls beider Computer erlauben, bevor Sie die Verbindung zwischen den IPv6-Adressen der Computer mit Ping überprüfen können. Hängen Sie bei Bedarf die Schnittstellen-ID an die IPv6-Schnittstellenadresse an, um sicherzustellen, dass die Adresse auf der richtigen Schnittstelle konfiguriert ist. Abbildung 6.22 weiter oben in dieser Lektion zeigt den Aufruf von Ping mit einer IPv6-Adresse und einer Schnittstellen-ID.

Wenn Sie die Konnektivität zu einem Host in einem Remotenetzwerk prüfen, sollten Sie als Erstes den Zielcache testen und löschen, der die IPv6-Adressen für Ziele des nächsten Abschnitts speichert. Den aktuellen Inhalt des Zielcaches zeigen Sie mit dem Befehl `netsh interface ipv6 show destinationcache` an. Der Befehl `netsh interface ipv6 delete destinationcache` löscht den Cache. Auch hier gilt, dass Sie die Eingabeaufforderung als Administrator ausführen müssen.

Im nächsten Schritt sollten Sie die Konnektivität zur Standardrouterschnittstelle in Ihrem lokalen Subnetz prüfen. Dies ist Ihr Standardgateway. Die IPv6-Adresse Ihrer Standardrouterschnittstelle finden Sie mit den Befehlen `ipconfig`, `netsh interface ipv6 show routes` oder `route print` heraus. Sie können auch die Zonen-ID angeben; dies ist die Schnittstellen-ID für das Standardgateway auf der Schnittstelle, auf der Sie die ICMPv6-Echo-Request-Nachrichten senden wollen. Wenn Sie sichergestellt haben, dass das Standardgateway in Ihrem lokalen Subnetz erreichbar ist, sollten Sie den Remotehost anhand seiner IPv6-Adresse mit Ping testen. Beachten Sie, dass Sie keinen Ping-Test auf die verbindungslokale IPv6-Adresse eines Remotehosts (oder einer Routerschnittstelle) durchführen können, weil verbindungslokale Adressen nicht routingfähig sind.

Wenn Sie eine Verbindung zum Standardgateway haben, aber die Remotezieladresse nicht erreichen, sollten Sie die Route zum Remoteziel verfolgen, indem Sie den Befehl `tracert -d` gefolgt von der Ziel-IPv6-Adresse eingeben. Das Befehlszeilenargument `-d` verhindert, dass Tracert eine DNS-Reverseabfrage für die Routerschnittstellen im Routingpfad durchführt. Auf diese Weise wird der Routingpfad schneller angezeigt. Wenn Sie mehr Informationen über die Router im Pfad brauchen und vor allem, wenn Sie die Routerzuverlässigkeit überprüfen wollen, sollten Sie den Befehl `pathping -d` gefolgt von der Ziel-IPv6-Adresse eingeben.

Schnelltest

- Mit welchem Netsh-Befehl ermitteln Sie die IPv6-Adresse Ihrer Standardrouterschnittstelle?

Antwort zum Schnelltest

- `netsh interface ipv6 show route`

Beseitigen von Konnektivitätsproblemen

Falls es Ihnen nicht gelingt, eine Verbindung zu einem Remotehost herzustellen, sollten Sie zuerst einmal die verschiedenen Hardwareverbindungen (Kabel und drahtlos) in Ihrer Organisation prüfen und sicherstellen, dass alle Netzwerkgeräte laufen. Decken diese einfachen Überprüfungen kein Problem auf, ist unter Umständen IPSec (Internet Protocol Security) falsch konfiguriert oder es bestehen Firewallprobleme (beispielsweise falsch konfigurierte Paketfilter).

Mit der Konsole *IP-Sicherheitsrichtlinienverwaltung* (Abbildung 6.26) prüfen und konfigurieren Sie die IPSec-Richtlinien, und mit der Konsole *Windows-Firewall mit erweiterter Sicherheit* (siehe Abbildung 6.11 und 6.12 in Lektion 1) prüfen und konfigurieren Sie IPv6-Paketfilter.

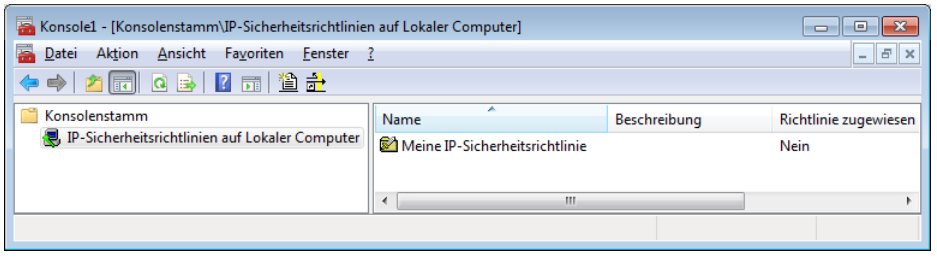


Abbildung 6.26 Die Konsole *IP-Sicherheitsrichtlinienverwaltung*



Hinweis IPSec6

Das Tool IPSec6 steht in Windows 7 nicht zur Verfügung.

Möglicherweise lässt sich keine Verbindung zu einem lokalen oder Remoteziel herstellen, weil Routen in der lokalen IPv6-Routingtabelle fehlen oder falsch sind. Mit den Befehlen `route print`, `netstat -r` oder `netsh interface ipv6 show route` zeigen Sie die lokale IPv6-Routingtabelle an, sodass Sie überprüfen können, ob eine Route für Ihr lokales Subnetz und zu

Ihrem Standardgateway vorhanden ist. Die Befehle `netstat -r` und `route print` zeigen sowohl die IPv4- als auch die IPv6-Routingtabellen an.

Übung Konfigurieren der IPv6-Konnektivität

In dieser Übung richten Sie eine statische standortlokale IPv6-Konfiguration auf dem Windows 7-Computer *Canberra* ein. Dann konfigurieren Sie eine statische standortlokale IPv6-Adresse auf dem Windows 7-Computer *Aberdeen* und testen die IPv6-Konnektivität.

Übung 1 Konfigurieren von IPv6 auf dem Computer *Canberra*

In dieser Übung konfigurieren Sie IPv6 auf dem Computer *Canberra*.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Erlauben Sie ICMPv6-Verkehr durch die Firewall von *Canberra*, indem Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen und den Befehl **netsh advfirewall firewall add rule name="ICMPv6" protocol=icmpv6:any,any dir=in action=allow** ausführen.
3. Öffnen Sie das Netzwerk- und Freigabecenter und klicken Sie auf *Adaptereinstellungen ändern*.
4. Klicken Sie mit der rechten Maustaste auf die Netzwerkverbindung mit Ihrem privaten Netzwerk und wählen Sie den Befehl *Eigenschaften*.
5. Wählen Sie *Internetprotokoll Version 6 (TCP/IPv6)* aus und klicken Sie auf *Eigenschaften*.
6. Tragen Sie die statische standortlokale IPv6-Adresse fec0:0:0:fffe::1 ein.
7. Klicken Sie in das Textfeld *Subnetzpräfixlänge*. Der Wert 64 wird automatisch eingetragen. Das Eigenschaftendialogfeld müsste nun ähnlich wie in Abbildung 6.27 aussehen.

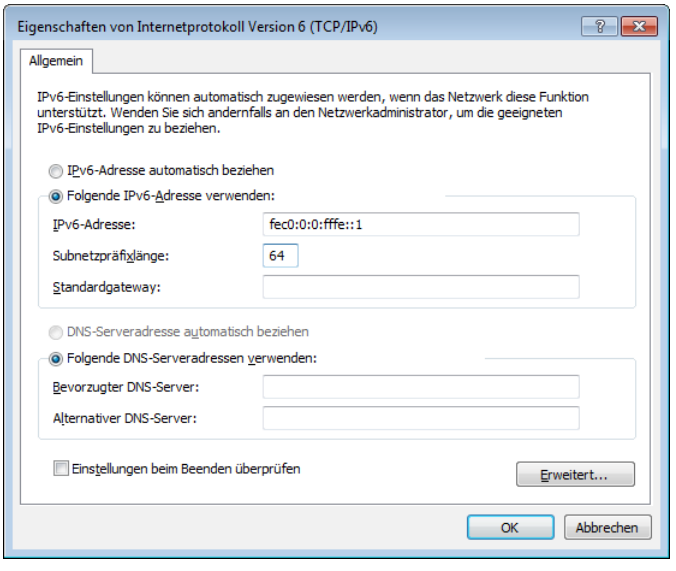


Abbildung 6.27 IPv6-Konfiguration auf dem Computer *Canberra*

8. Klicken Sie auf *OK*. Schließen Sie das Dialogfeld *Eigenschaften von LAN-Verbindung*.
9. Schließen Sie das Netzwerk- und Freigabecenter.
10. Geben Sie in der Eingabeaufforderung mit erhöhten Rechten **ping fec0:0:0:fffe::1** ein. Ihr Bildschirm müsste nun ähnlich aussehen wie in Abbildung 6.28.

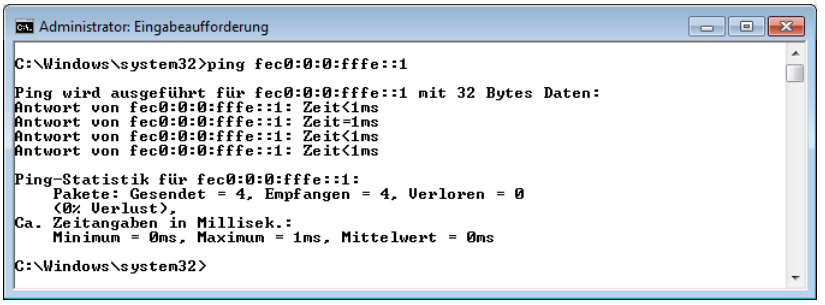

Administrator: Eingabeaufforderung
C:\Windows\system32>ping fec0:0:0:fffe::1
Ping wird ausgeführt für fec0:0:0:fffe::1 mit 32 Bytes Daten:
Antwort von fec0:0:0:fffe::1: Zeit<1ms
Antwort von fec0:0:0:fffe::1: Zeit=1ms
Antwort von fec0:0:0:fffe::1: Zeit<1ms
Antwort von fec0:0:0:fffe::1: Zeit<1ms
Ping-Statistik für fec0:0:0:fffe::1:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms
C:\Windows\system32>

Abbildung 6.28 Ping-Test mit einer standortlokalen IPv6-Adresse

Übung 2 Konfigurieren des Computers *Aberdeen* und Testen der IPv6-Konnektivität

In dieser Übung richten Sie auf dem Computer *Aberdeen* eine standortlokale IPv6-Adresse ein und testen die Konnektivität. Sie müssen die IPv6-Einstellungen auf dem Computer *Canberra* konfiguriert haben, bevor Sie diese Übung beginnen. Falls Aberdeen ein virtueller Computer ist, hat der Ethernetadapter, der mit Ihrem privaten Netzwerk verbunden ist, unter Umständen einen anderen Namen als *LAN-Verbindung*. Passen Sie die Befehle in diesem Fall entsprechend an.

1. Melden Sie sich mit dem Konto *Kim_Akers* am Computer *Aberdeen* an.
2. Erlauben Sie ICMPv6-Verkehr durch die Firewall von *Aberdeen*, indem Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen und den Befehl **netsh advfirewall firewall add rule name="ICMPv6" protocol=icmpv6:any,any dir=in action=allow** ausführen.
3. Konfigurieren Sie eine statische IPv6-Adresse, indem Sie **netsh interface ipv6 set address "local area connection" fec0:0:0:fffe::a** eingeben.
4. Geben Sie **ping fec0:0:0:fffe::a** ein, um Ihre IPv6-Konfiguration zu testen.
5. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen, und öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.

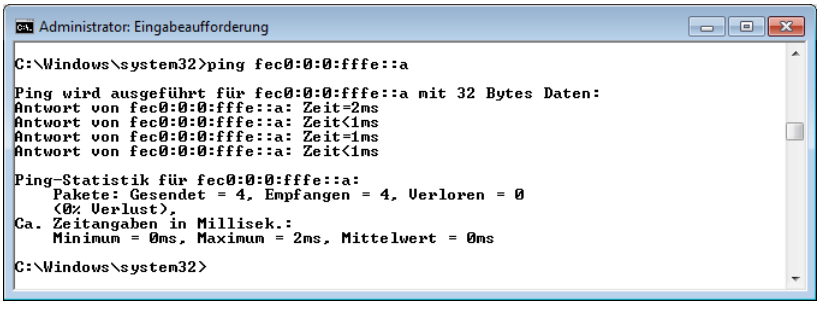

Administrator: Eingabeaufforderung
C:\Windows\system32>ping fec0:0:0:fffe::a
Ping wird ausgeführt für fec0:0:0:fffe::a mit 32 Bytes Daten:
Antwort von fec0:0:0:fffe::a: Zeit=2ms
Antwort von fec0:0:0:fffe::a: Zeit<1ms
Antwort von fec0:0:0:fffe::a: Zeit=1ms
Antwort von fec0:0:0:fffe::a: Zeit<1ms
Ping-Statistik für fec0:0:0:fffe::a:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 2ms, Mittelwert = 0ms
C:\Windows\system32>

Abbildung 6.29 Ping-Test von *Canberra* zum Computer *Aberdeen*

6. Geben Sie **ping fec0:0:0:fffe::a** ein. Der Test müsste erfolgreich verlaufen, wie in Abbildung 6.29 gezeigt.
7. Geben Sie **netsh interface ipv6 show neighbors** ein. Abbildung 6.30 zeigt die Schnittstelle fec0:0:0:fffe::a als Nachbarn im selben Subnetz wie der Computer *Canberra*.

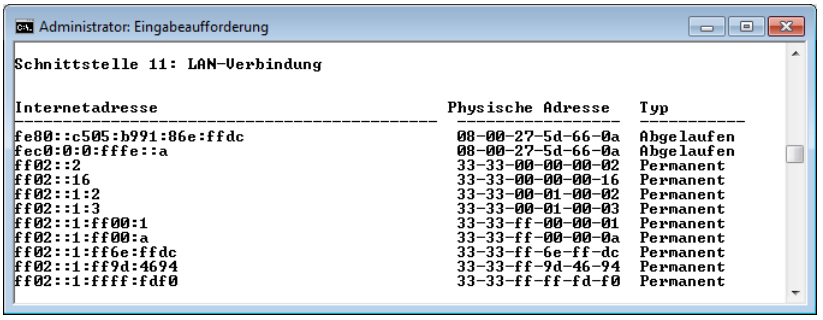


Abbildung 6.30 Anzeigen der Nachbarn des Computers *Canberra*

Zusammenfassung der Lektion

- IPv6 unterstützt Unicast-, Multicast- und Anycastadressen. Unicastadressen können global, standortlokal, verbindungslokal oder speziell sein.
- IPv6 wird in Windows 7 vollständig unterstützt. Es beseitigt etliche Probleme von IPv4, etwa den beschränkten Adressraum.
- IPv6 ist so entworfen, dass es abwärtskompatibel ist. Sie können IPv4-kompatible Adressen verwenden, beispielsweise Teredo- und 6to4-Adressen.
- Als Tools für die Konfiguration und Problembehandlung von IPv6 stehen unter anderem Ping, Ipconfig, Tracert, Pathping und Netsh zur Verfügung.
- Sie können IPv6 über die GUI des TCP/IPv6-Eigenschaftendialogfelds konfigurieren. In der Eingabeaufforderung stehen die Befehle von `netsh interface ipv6` zur Verfügung, um IPv6-Einstellungen zu konfigurieren.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Konfigurieren von IPv6«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welchen Typ Unicast-IPv6-Adresse verwenden Sie normalerweise in den Subnetzen eines privaten Netzwerks, um IPv6-Konnektivität im gesamten Subnetz zu implementieren?

A. Standortlokale Adresse
B. Verbindungslokale Adresse
C. Spezielle Adresse
D. Anycastadresse

2. Sie analysieren die Konfiguration eines IPv6-Netzwerks. Welche der folgenden Adressen kann im IPv6-Internet benutzt werden und ist das Gegenstück zu einer öffentlichen Unicastadresse in IPv4?
   A. fec0:0:0:0:fffe::1
   B. 21cd:53::3ad:3f:af37:8d62
   C. fe80:d1ff:d166:7888:2fd6
   D. ::1
3. Sie analysieren mit dem Network Monitor den Verkehr in einem IPv6-Netzwerk. Sie wollen das Protokoll untersuchen, das mithilfe von ICMPv6-Nachrichten die Interaktion benachbarter Knoten verwaltet und IPv6-Adressen in Hardwareadressen (MAC-Adressen) auflöst. Welches Protokoll untersuchen Sie?
   A. ARP
   B. DNS
   C. DHCPv6
   D. ND
4. Sie untersuchen Übergangstechnologien in einem Netzwerk und wollen herausfinden, welche Adressen aus dem Bereich der IPv4-zu-IPv6-Kompatibilität benutzt werden. Welche der folgenden ist eine Teredo-Adresse?
   A. 2001::0a0a:1efe:e866:efff:f5ff:ebfe
   B. 2002:c058:6301::
   C. fe80::5efe:0a00:028f
   D. fec0:0:0:0:fffe::1
5. Sie untersuchen eine DNS-Forward-Lookupzone, um Probleme mit der Namensauflösung zu beseitigen. Welcher Art Ressourceneintrag ermöglicht es DNS, einen Hostnamen in eine IPv6-Adresse aufzulösen?
   A. PTR
   B. A
   C. AAAA
   D. Host

Lektion 3: Netzwerkkonfiguration

Als IT-Experte sind Sie hauptsächlich damit beschäftigt, Produktivnetzwerke einzurichten und zu administrieren, die Domänencontroller, Dateiserver, DNS-Server, DHCP-Server, Computer mit Exchange Server, Computer mit Microsoft SQL Server und ähnliche Dienste enthalten. Aber auch große Organisationen richten oft für spezielle Zwecke kleine Netzwerke ein (zum Beispiel Testnetzwerke). Vielleicht müssen Sie auch eine Arbeitsgruppe einrichten, die ICS benutzt, oder Drahtlosverbindungen konfigurieren.

Diese Lektion beschreibt, wie Sie Geräte in Kabel- und Drahtlosnetzwerken einrichten, vor allem konzentriert sie sich aber auf Drahtlosnetzwerke. Sie erklärt, wie Sie Sicherheitseinstellungen auf einem Client konfigurieren, die bevorzugten Drahtlosnetzwerke verwalten, Drahtlosnetzwerkadapter konfigurieren und spezielle Konnektivitätsprobleme von Drahtlosadaptern beseitigen. Außerdem behandelt diese Lektion die Sicherheitseinstellungen in einem WAP und erklärt, wie Sie standortabhängiges Drucken konfigurieren.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Verbinden von Arbeitsstationen mit einem Kabelnetzwerk
- Hinzufügen eines Geräts zu einem Drahtlosnetzwerk
- Verwalten von Verbindungen in Kabel- und Drahtlosnetzwerken
- Verwalten bevorzugter Drahtlosnetzwerke
- Konfigurieren der Sicherheitseinstellungen im WAP eines anderen Herstellers
- Konfigurieren des standortabhängigen Druckens

Veranschlagte Zeit für diese Lektion: 50 Minuten

Herstellen der Verbindung zu einem Netzwerk

Lektion 1 hat beschrieben, wie Sie ein kleines Kabelnetzwerk einrichten, in dem ein Computer direkt mit einem DSL- oder DFÜ-Modem verbunden ist und seine IPv4-Konfiguration von diesem Modem erhält. Das Modem wird dabei vom Internetprovider konfiguriert. Ein solcher Computer wird üblicherweise so konfiguriert, dass er ICS zur Verfügung stellt. Weitere Clients, die Sie mit dem Netzwerk verbinden, erhalten ihre Konfigurationen dann automatisch vom ICS-Computer. Abbildung 6.31 zeigt diese Konfiguration.

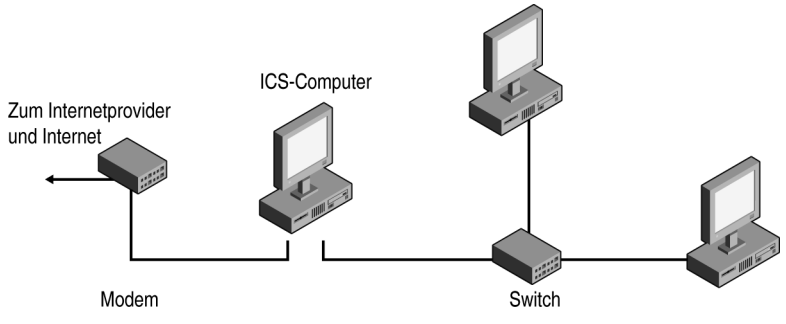


Abbildung 6.31 Ein kleines Kabelnetzwerk

In einem kleinen Drahtlosnetzwerk verbinden Sie Ihren Drahtloszugriffspunkt (Wireless Access Point, WAP) mit Ihrem DSL- oder DFÜ-Modem. Die anderen Geräte in Ihrem Netzwerk, etwa Computer oder Drucker, stellen dann die Verbindung zum WAP her. In diesem Fall greifen die Computer im Netzwerk über den WAP auf das Internet zu, der in der Standardeinstellung so konfiguriert ist, dass er IP-Konfigurationen zuweist. Abbildung 6.32 zeigt diese Konfiguration. Wenn Sie das Netzwerk ganz neu einrichten, Ihr Internetprovider aber kein Modem zur Verfügung stellt, können Sie ein Kombimodell aus Modem und WAP kaufen.

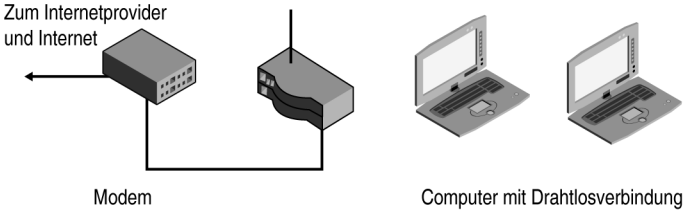


Abbildung 6.32 Ein kleines Drahtlosnetzwerk

Sie können auch ein hybrides Netzwerk implementieren. In diesem Fall ist der WAP meist wie vorher beschrieben mit dem Modem verbunden und die fest installierten Computer sind über Kabelverbindungen an Ethernetanschlüsse des WAPs angeschlossen. Die meisten WAPs haben neben dem WAN-Anschluss (Wide Area Network), der die Verbindung zum Modem liefert, noch mehrere Ethernetanschlüsse. Sie können die Desktopcomputer direkt an den WAP anschließen oder an einen Ethernetswitch (oder Hub), der dann wiederum mit dem WAP verbunden ist. Drahtlosgeräte verbinden sich direkt mit dem WAP. Kabelgebundene und Drahtlosgeräte befinden sich im selben Netzwerk und beziehen ihre IP-Konfiguration vom WAP, der DHCP und interne DNS-Dienste zur Verfügung stellt. Abbildung 6.33 zeigt diese Konfiguration.

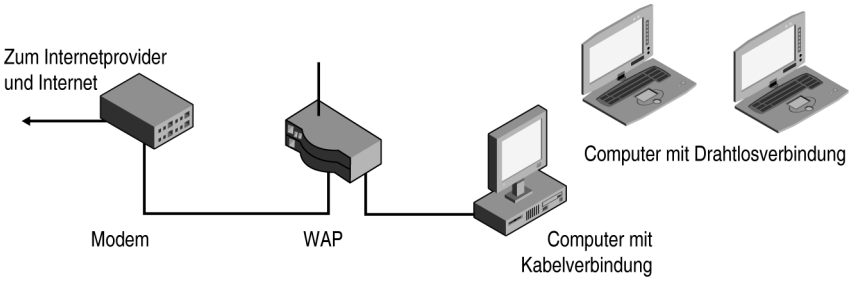


Abbildung 6.33 Ein kleines Hybridnetzwerk

Der WAP leitet alle Pakete, die ins Internet gerichtet sind (beispielsweise Browseranforderungen), über das Modem an Ihren Internetprovider, der die DNS-Auflösung im Internet durchführt. Normalerweise konfigurieren Sie den WAP, indem Sie auf eine Weboberfläche zugreifen. Einzelheiten finden Sie in der Dokumentation des Herstellers.

Weitere Informationen Externe Auflösung

Es ist unwahrscheinlich, dass Sie in Prüfung 70-680 Fragen zur Funktionsweise von DNS im Internet beantworten müssen. Wenn Sie sich für das Thema interessieren, können Sie sich unter *http://technet.microsoft.com/de-de/library/cc775637.aspx* genauer informieren.

Wenn Sie mehrere Drahtloscomputer sehr nah beieinander aufgestellt haben (höchstens 10 Meter Abstand), können Sie ein Ad-hoc-Netzwerk einrichten, das es ermöglicht, auf freigegebene Ressourcen der Computer im Netzwerk zuzugreifen (sofern die entsprechenden Freigabeberechtigungen vorhanden sind). Ein Ad-hoc-Netzwerk benötigt keinen zentralen WAP und braucht keine IPv4-Konfiguration, weil es mit IPv6 arbeitet. Ad-hoc-Netzwerke werden weiter unten in dieser Lektion genauer beschrieben. In einer der Übungen richten Sie außerdem ein Ad-hoc-Netzwerk ein.

Einrichten einer Netzwerkverbindung

Der erste Computer, den Sie in einem Test- oder SOHO-Kabelnetzwerk installieren, ist normalerweise über eine USB- (Universal Serial Bus) oder Ethernetverbindung an das Modem angeschlossen. Er hat außerdem eine Ethernetverbindung, über die Computer und andere Geräte eine Verbindung über einen Switch herstellen können. Ihr Internetprovider erklärt Ihnen, wie Sie eine Internetverbindung herstellen, und gibt Ihnen einen Benutzernamen und das zugehörige Kennwort.

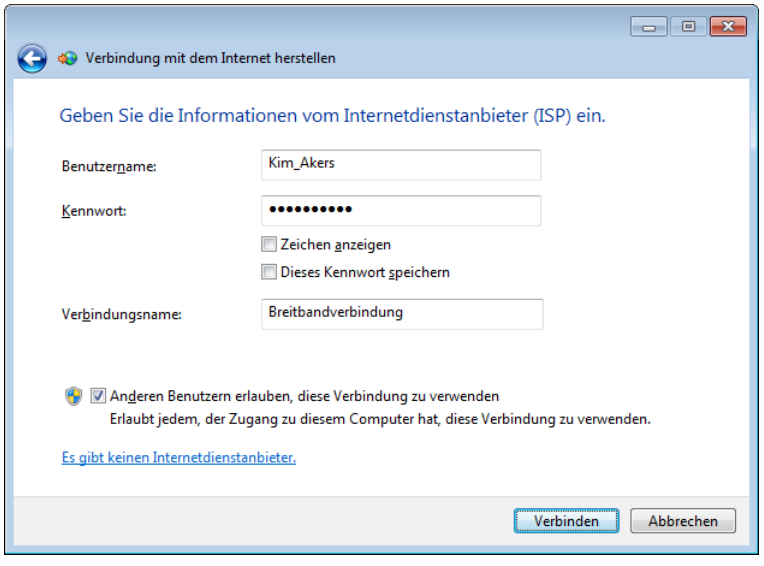


Abbildung 6.34 Eingeben der vom Internetprovider erhaltenen Zugangsinformationen

Sie richten eine Verbindung ins Internet ein, indem Sie das Netzwerk- und Freigabecenter öffnen. Klicken Sie auf *Neue Verbindung oder neues Netzwerk einrichten*, dann auf *Verbindung mit dem Internet herstellen* und schließlich auf *Weiter*. Sie können jetzt auswählen, auf welche Art die Verbindung hergestellt wird, zum Beispiel eine Breitband-PPPoE-Verbindung (Point-To-Point Protocol Over Ethernet). Geben Sie auf der nächsten Seite Ihren Namen und das Kennwort ein, die Ihr Internetprovider Ihnen genannt hat (Abbildung 6.34). Wenn Sie

das Kontrollkästchen *Anderen Benutzern erlauben, diese Verbindung zu verwenden* aktivieren, aber nicht unter einem Administratorkonto angemeldet sind, werden Sie aufgefordert, entsprechende Anmeldeinformationen einzugeben.

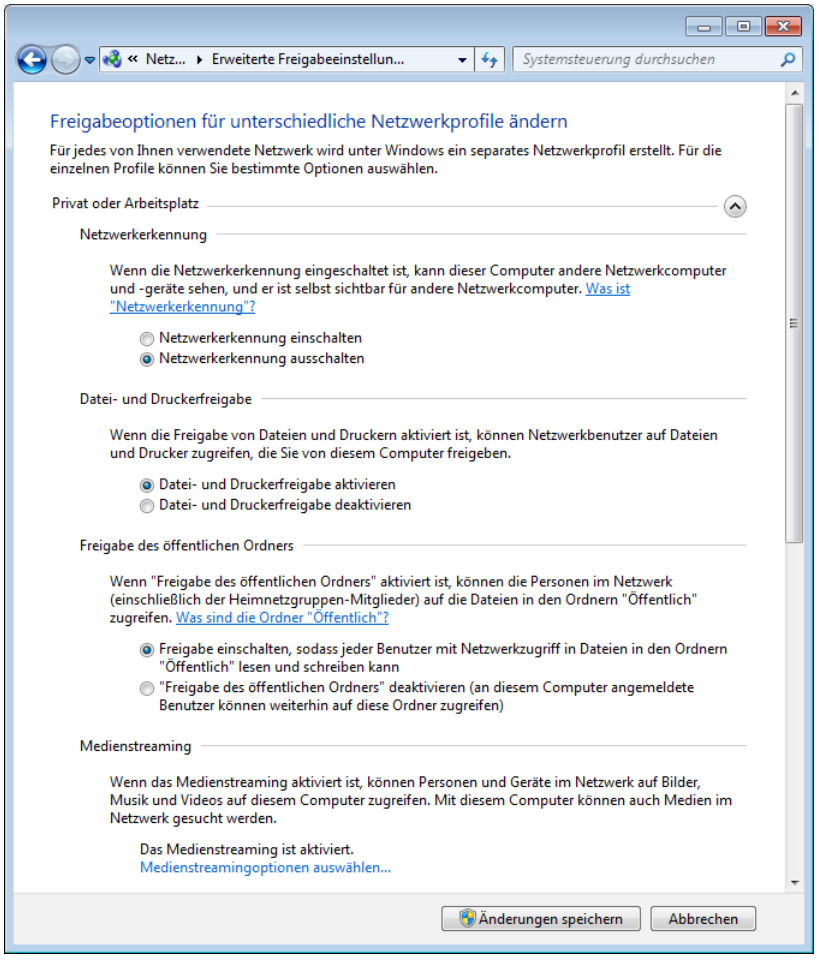

« Netz... ▸ Erweiterte Freigabeeinstellun...
Systemsteuerung durchsuchen
Freigabeoptionen für unterschiedliche Netzwerkprofile ändern
Für jedes von Ihnen verwendete Netzwerk wird unter Windows ein separates Netzwerkprofil erstellt. Für die einzelnen Profile können Sie bestimmte Optionen auswählen.
Privat oder Arbeitsplatz
Netzwerkerkennung
Wenn die Netzwerkerkennung eingeschaltet ist, kann dieser Computer andere Netzwerkcomputer und -geräte sehen, und er ist selbst sichtbar für andere Netzwerkcomputer. Was ist "Netzwerkerkennung"?
Netzwerkerkennung einschalten
Netzwerkerkennung ausschalten
Datei- und Druckerfreigabe
Wenn die Freigabe von Dateien und Druckern aktiviert ist, können Netzwerkbenutzer auf Dateien und Drucker zugreifen, die Sie von diesem Computer freigeben.
Datei- und Druckerfreigabe aktivieren
Datei- und Druckerfreigabe deaktivieren
Freigabe des öffentlichen Ordners
Wenn "Freigabe des öffentlichen Ordners" aktiviert ist, können die Personen im Netzwerk (einschließlich der Heimnetzgruppen-Mitglieder) auf die Dateien in den Ordnern "Öffentlich" zugreifen. Was sind die Ordner "Öffentlich"?
Freigabe einschalten, sodass jeder Benutzer mit Netzwerkzugriff in Dateien in den Ordnern "Öffentlich" lesen und schreiben kann
"Freigabe des öffentlichen Ordners" deaktivieren (an diesem Computer angemeldete Benutzer können weiterhin auf diese Ordner zugreifen)
Medienstreaming
Wenn das Medienstreaming aktiviert ist, können Personen und Geräte im Netzwerk auf Bilder, Musik und Videos auf diesem Computer zugreifen. Mit diesem Computer können auch Medien im Netzwerk gesucht werden.
Das Medienstreaming ist aktiviert.
Medienstreamingoptionen auswählen...
Änderungen speichern
Abbrechen

Abbildung 6.35 Das Dialogfeld *Erweiterte Freigabeeinstellungen*

Sie können sich Details zu den Freigabe- und Netzwerkerkennungseinstellungen ansehen und die Einstellungen bei Bedarf ändern, indem Sie auf *Erweiterte Freigabeeinstellungen ändern* klicken. Abbildung 6.35 zeigt das Dialogfeld *Erweiterte Freigabeeinstellungen*. Sie können hier die Einstellungen für ein öffentliches oder privates Profil (*Privat oder Arbeitsplatz*) ändern, indem Sie auf die Pfeilschaltfläche rechts neben dem aktuellen Profil klicken. Bei jedem Profil können Sie folgende Einstellungen konfigurieren:

- Netzwerkerkennung
- Datei- und Druckerfreigabe
- Freigabe des öffentlichen Ordners
- Medienstreaming

- Dateifreigabeverbindungen (Verschlüsselungsstärke)
- Kennwortgeschütztes Freigeben
- Heimnetzgruppen-Verbindungen

Normalerweise stellen andere Computer in einem kleinen Kabelnetzwerk die Internetverbindung über den ersten Computer her, den Sie im Netzwerk konfigurieren. Damit das geschieht, müssen Sie ICS auf diesem Computer konfigurieren. In Übung 2, »Konfigurieren von ICS auf dem Computer *Canberra*«, von Lektion 1 haben Sie einen ICS-Computer und einen ICS-Client konfiguriert.

Wenn Sie ICS aktivieren, wird Ihre LAN-Verbindung mit einer neuen statischen IP-Adresse (192.168.0.1) und anderen Einstellungen konfiguriert, darunter Subnetzmaske, Standardgateway und DNS-Serveradresse. Die statische Adresse (192.168.0.1) wird als Standardgateway für das Subnetz verwendet. Wenn Sie andere Computer mit Ihrem Netzwerk verbinden, bevor Sie ICS aktivieren, müssen Sie unter Umständen deren TCP/IP-Einstellungen verändern. Üblicherweise starten Sie die Computer dazu neu. Generell ist es sinnvoller, andere Computer erst zu Ihrem Netzwerk hinzuzufügen, nachdem Sie ICS konfiguriert haben.

Um einen Computer zu einem Kabelnetzwerk hinzuzufügen, in dem ICS konfiguriert ist, brauchen Sie ihn lediglich an das Netzwerk anzuschließen und anzuschalten. Klicken Sie im Netzwerk- und Freigabecenter auf *Internetoptionen*, dann auf der Registerkarte *Verbindungen* auf *LAN-Einstellungen* und deaktivieren Sie das Kontrollkästchen *Automatische Suche der Einstellungen*. Sofern der Netzwerkadapter des Computers so konfiguriert ist, dass er seine Konfiguration automatisch bezieht, und der Name des Computers nicht bereits von einem anderen Computer im Netzwerk verwendet wird, tritt der Computer dem Netzwerk bei und erhält seine Konfiguration über ICS. Falls Sie den Standardnamen für die Arbeitsgruppe (*WORKGROUP*) in Ihrem Netzwerk geändert haben, müssen Sie auch diese Einstellung auf allen Computern anpassen, die Sie hinzufügen wollen.

Wenn Sie einen Computer über eine Kabelverbindung an ein hybrides Netzwerk anschließen, ist das sogar noch einfacher als bei einem reinen Kabelnetzwerk. Sie stecken ihn einfach an und schalten ihn ein. In der Standardeinstellung müsste er so konfiguriert sein, dass er seine IP-Einstellungen automatisch bezieht. In diesem Fall bekommt er sie allerdings vom WAP.

Hinzufügen eines Drahtloscomputers zu einem Netzwerk

Wenn Sie einen drahtlosfähigen Computer haben, können Sie auf das Netzwerksymbol im Infobereich Ihrer Taskleiste rechts unten auf dem Bildschirm klicken. Daraufhin werden alle Drahtlosnetzwerke aufgelistet, die sich in Reichweite befinden, und Sie können doppelt auf das Netzwerk klicken, zu dem Sie eine Verbindung herstellen wollen. Stattdessen können Sie auch das Netzwerk- und Freigabecenter öffnen und auf *Verbindung mit einem Netzwerk herstellen* klicken. Den Verbindungsstatus können Sie anzeigen und ändern, indem Sie neben *Aktive Netzwerke anzeigen* im Netzwerk- und Freigabecenter auf *Verbindung herstellen oder trennen* klicken. Es öffnet sich dann wiederum die Liste mit allen Drahtlosnetzwerken, die in Reichweite sind.

Auch in der Befehlszeile können Sie einen Computer mit einem Drahtlosnetzwerk verbinden. Der folgende Befehl zeigt die verfügbaren Drahtlosschnittstellen an:

```
netsh wlan show interfaces
```

Die Ausgabe dieses Befehls auf einem Computer, der nur eine Schnittstelle hat, sehen Sie in Abbildung 6.36.

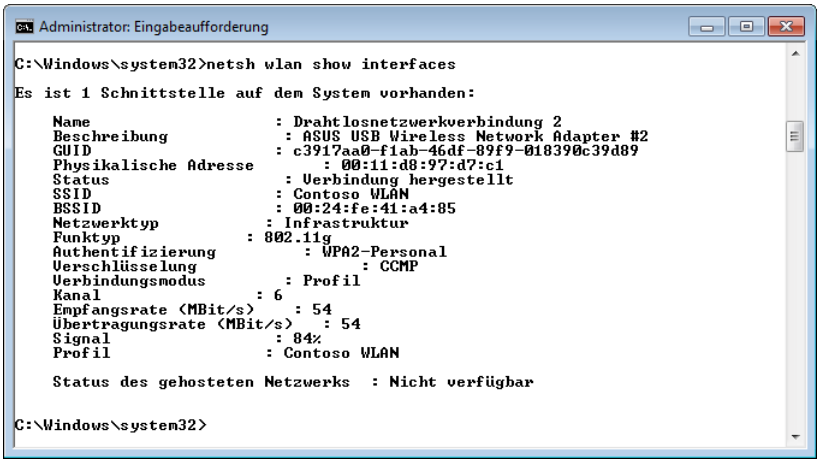


Abbildung 6.36 Drahtlosschnittstelle auf dem Computer *Canberra*

Um eine Verbindung zu dem Drahtlosnetzwerk herzustellen, das in Abbildung 6.36 aufgeführt wird, geben Sie folgenden Befehl ein:

```
netsh wlan connect name=default
```

Gibt es mehrere Drahtlosnetzwerke im selben Profil, müssen Sie zusätzlich die SSID (Service Set Identifier) des Netzwerks angeben, zu dem Sie eine Verbindung herstellen wollen. Haben Sie beispielsweise ein Ad-hoc-Netzwerk namens *MyOtherNet* eingerichtet, zu dem Sie nun eine Verbindung herstellen wollen, lautet der entsprechende Befehl:

```
netsh wlan connect name=default ssid=myothernet
```

Wenn Sie einen Befehl ausführen, um eine Verbindung zu einem Drahtlosnetzwerk herzustellen, Ihr Computer aber schon mit einem Drahtlosnetzwerk verbunden ist, trennt er die Verbindung zum bisherigen Netzwerk und baut eine neue Verbindung zum angegebenen Netzwerk auf. Wenn Sie die Verbindung zu einem Netzwerk trennen wollen, ohne sich mit einem anderen zu verbinden, können Sie den folgenden Befehl eingeben, sofern Sie nur einen Drahtlosadapter im Computer haben:

```
netsh wlan disconnect
```

Haben Sie mehrere Drahtlosschnittstellen in Ihrem System, müssen Sie die Schnittstelle angeben, deren Verbindung Sie trennen wollen. Der Befehl sieht dann beispielsweise so aus:

```
netsh wlan disconnect interface="Drahtlosnetzwerkverbindung"
```

Und der folgende Befehl trennt die Verbindungen aller Schnittstellen:

```
netsh wlan disconnect interface=*
```

Das Tool `netsh wlan` ist sowohl vielseitig als auch leistungsfähig. Wie bei allen Befehlszeilenprogrammen werden Sie am schnellsten damit vertraut, wenn Sie es ausgiebig benutzen und damit experimentieren. Dies ist eine der vorgeschlagenen Übungen am Ende des Kapitels. Abbildung 6.37 zeigt, welche Befehle für `netsh wlan` zur Verfügung stehen.

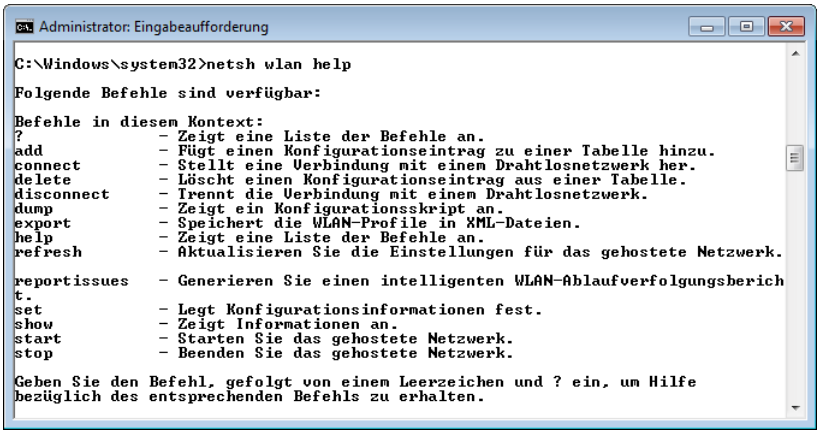

Administrator: Eingabeaufforderung
C:\Windows\system32>netsh wlan help
Folgende Befehle sind verfügbar:
Befehle in diesem Kontext:
? - Zeigt eine Liste der Befehle an.
add - Fügt einen Konfigurationseintrag zu einer Tabelle hinzu.
connect - Stellt eine Verbindung mit einem Drahtlosnetzwerk her.
delete - Löscht einen Konfigurationseintrag aus einer Tabelle.
disconnect - Trennt die Verbindung mit einem Drahtlosnetzwerk.
dump - Zeigt ein Konfigurationsskript an.
export - Speichert die WLAN-Profile in XML-Dateien.
help - Zeigt eine Liste der Befehle an.
refresh - Aktualisieren Sie die Einstellungen für das gehostete Netzwerk.
reportissues - Generieren Sie einen intelligenten WLAN-Ablaufverfolgungsbericht.
set - Legt Konfigurationsinformationen fest.
show - Zeigt Informationen an.
start - Starten Sie das gehostete Netzwerk.
stop - Beenden Sie das gehostete Netzwerk.
Geben Sie den Befehl, gefolgt von einem Leerzeichen und ? ein, um Hilfe bezüglich des entsprechenden Befehls zu erhalten.

Abbildung 6.37 Befehle von `netsh wlan`

Das Verhalten einer Drahtlosverbindung konfigurieren Sie, indem Sie im Netzwerk- und Freigabecenter *Adaptereinstellungen ändern* anklicken, mit der rechten Maustaste auf Ihren Drahtlosadapter klicken und den Befehl *Status* wählen. Klicken Sie im Dialogfeld *Status* auf *Details*, um die Adapterkonfiguration anzuzeigen (Abbildung 6.38).

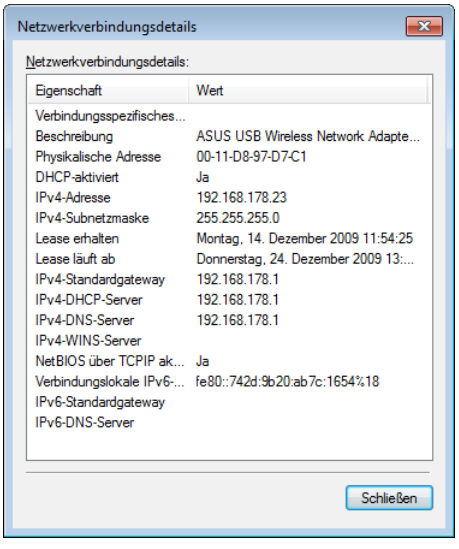


Abbildung 6.38 Konfiguration eines Drahtlosadapters

Wenn Sie im Dialogfeld *Status* eines Adapters auf *Drahtloseigenschaften* klicken, öffnet sich das Dialogfeld *Eigenschaften für Drahtlosnetzwerk* für das Drahtlosnetzwerk, mit dem Sie momentan verbunden sind (Abbildung 6.39). Sie können Ihren Computer so konfigurieren, dass er sich immer mit dem aktuellen Netzwerk verbindet, sobald es in Reichweite ist, oder eine Verbindung zu einem anderen Netzwerk aufbaut, das in der Liste der bevorzugten Netzwerke weiter oben steht. Sie können einen WAP so konfigurieren, dass er seinen Namen oder die SSID nicht aussendet. Das verbessert die Sicherheit, weil das Netzwerk nicht in der Liste der verfügbaren Drahtlosnetzwerke auftaucht und Sie von Hand eine Verbindung dazu

herstellen müssen. Sie können Ihren Computer (und somit auch andere Computer in Ihrem Netzwerk) so konfigurieren, dass er eine Verbindung zu einem Netzwerk herstellt, das sich in Reichweite befindet, aber nicht seine SSID aussendet. Sie können diese und andere Einstellungen auf ein USB-Flashlaufwerk kopieren, mit dem Sie dann andere Computer so konfigurieren, dass sie eine Verbindung zu Ihrem Drahtlosnetzwerk herstellen.

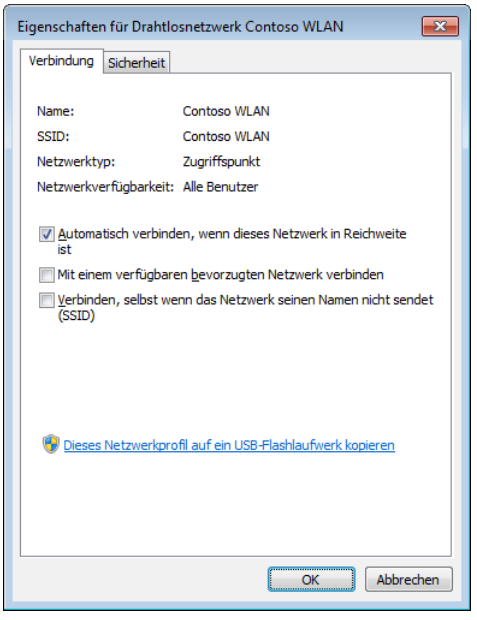


Abbildung 6.39 Konfigurieren der Verbindungseigenschaften

Wenn Sie das Kontrollkästchen *Mit einem verfügbaren bevorzugten Netzwerk verbinden* aktivieren, wird die automatische Umschaltung aktiviert. Das ist in großen Organisationen oft nützlich, wo mehrere Drahtlosnetzwerke gebraucht werden, um das Firmengelände abzudecken. Nehmen wir an, eine Ärztin bewegt sich mit ihrem Notebook von einer Krankenhausabteilung in eine andere. Sie will nicht jedes Mal, wenn sie den Bereich des aktuellen Drahtlosnetzwerks verlässt, von Hand die Verbindung zu einem anderen herstellen. Die automatische Umschaltung erledigt das nahtlos, ohne dass Benutzereingaben erforderlich sind.

Die automatische Umschaltung kann allerdings auch Probleme verursachen, wenn sich zwei Netzwerke überschneiden. Das wird im Abschnitt »Problembehandlung für Drahtlosnetzwerke« weiter unten in dieser Lektion genauer beschrieben.

Sie können zusätzliche drahtlosfähige Computer zu Ihrem Netzwerk hinzufügen, indem Sie das USB-Flashlaufwerk einstecken und im Dialogfeld *Automatische Wiedergabe* auf *Drahtlosnetzwerkinstallations-Assistent* klicken. Stattdessen können Sie einen drahtlosfähigen Windows 7-Computer auch von Hand zu Ihrem Netzwerk hinzufügen, indem Sie im Netzwerk- und Freigabecenter auf *Verbindung mit einem Netzwerk herstellen* klicken und genauso vorgehen wie beim Verbinden des ersten Computers.



Hinweis Netzwerksicherheitsschlüssel

In der Standardeinstellung wird ein WAP so eingerichtet, dass er allen drahtlosfähigen Computern innerhalb seiner Reichweite den Zugriff erlaubt. Sie können sowohl Authentifizierungs- als auch Verschlüsselungstyp auf der Registerkarte *Sicherheit* im Dialogfeld *Eigenschaften für Drahtlosnetzwerk* konfigurieren. Wie Sie Sicherheitseinstellungen im WAP eines anderen Herstellers konfigurieren, wird weiter unten in dieser Lektion beschrieben.

Schnelltest

- Sie fügen einen neuen Computer zu einem Kabelnetzwerk hinzu. Dieses Netzwerk ist über ein DSL-Modem mit dem Internet verbunden. Das Modem ist über ein USB-Kabel an einen Ihrer Computer angeschlossen. Der neue Computer ist so konfiguriert, dass er seine IP-Konfiguration automatisch bezieht. Wenn Sie den neuen Computer anschalten, wird er mit einer IP-Adresse, einer Subnetzmaske und den IP-Adressen von Standardgateway und DNS-Server konfiguriert. Woher bekommt er diese Informationen?

Antwort zum Schnelltest

- Aus dem Computer, der an das Modem angeschlossen ist. Dieser Computer ist so konfiguriert, dass er ICS ausführt.

Wenn Sie eine Verbindung zu einem Drahtlosnetzwerk herstellen wollen, das seine SSID nicht aussendet, müssen Sie seine Daten kennen, beispielsweise Netzwerkname und Sicherheitstyp. Klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*, dann auf *Manuell mit einem Drahtlosnetzwerk verbinden* und schließlich auf *Weiter*. Sie werden nun aufgefordert, den Netzwerknamen und Sicherheitstyp sowie (sofern nötig) den Verschlüsselungstyp und den Sicherheitsschlüssel einzugeben. Stattdessen können Sie auch eine Eingabeaufforderung mit erhöhten Rechten öffnen und einen Befehl mit der folgenden Syntax ausführen:

```
netsh wlan connect name=<Profilname> ssid-<Netzwerk-SSID> [interface=<Schnittstellenname>]
```

Wenn Sie ein anderes Drahtlosgerät als einen Computer zu einem Netzwerk hinzufügen wollen, müssen Sie die Anleitungen des Herstellers befolgen, die im Handbuch des Geräts beschrieben sind. Unter Umständen können Sie das Gerät mithilfe eines USB-Flashlaufwerks zum Netzwerk hinzufügen. Falls das Gerät ein Drucker ist, müssen Sie möglicherweise die Druckerfreigabe aktivieren, damit andere Computer im Netzwerk ihn benutzen können. Falls Sie ein Bluetooth-fähiges Gerät zu Ihrem Netzwerk hinzufügen wollen, brauchen Sie eine Bluetooth-Netzwerkkarte.



Weitere Informationen Bluetooth

Weitere Informationen über Bluetooth finden Sie unter *http://bluetooth.com/Bluetooth/Technology/*. Klicken Sie dort auf die angebotenen Links.



Hinweis Virtuelle private Netzwerke

Sie können auch eine Verbindung zu einem virtuellen privaten Netzwerk (Virtual Private Network, VPN) herstellen, indem Sie im Netzwerk- und Freigabecenter auf *Verbindung mit einem Netzwerk herstellen* klicken. Kapitel 10, »DirectAccess und VPN-Verbindungen«, beschreibt VPNs genauer.

Verwalten der bevorzugten Drahtlosnetzwerke

Wenn Sie einen drahtlosfähigen mobilen Computer haben, beispielsweise ein Notebook, können Sie ihn an unterschiedliche Orte mitnehmen und jeweils mit dem vorhandenen Drahtlosnetzwerk verbinden. Welche Netzwerke vorhanden sind, können Sie sich ansehen, indem Sie das Netzwerk- und Freigabecenter öffnen und auf *Verbindung mit einem Netzwerk herstellen* klicken. Stattdessen können Sie auch auf das Drahtlossymbol im Infobereich der Taskleiste rechts unten auf dem Bildschirm klicken. Klicken Sie dann mit der rechten Maustaste auf ein Netzwerk und wählen Sie den Befehl *Verbinden*. Die verfügbaren Netzwerke werden im Dialogfeld *Drahtlosnetzwerke verwalten* aufgelistet.

Falls das Netzwerk, zu dem Sie eine Verbindung herstellen wollen, nicht angezeigt wird, können Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten* klicken. Sie bekommen eine Liste der verfügbaren Optionen angeboten (zum Beispiel *Verbindung mit dem Internet herstellen*) und können von Hand nach einem Netzwerk suchen und die Verbindung dazu herstellen. Sie können hier auch eine neue Netzwerkverbindung anlegen.

Manche Netzwerke benötigen einen Netzwerksicherheitsschlüssel oder eine Passphrase. Um die Verbindung zu einem sicheren Netzwerk herzustellen, das Sie nicht selbst verwalten, müssen Sie sich vom Netzwerkadministrator oder dem Dienstanbieter den Schlüssel oder die Passphrase geben lassen.



Warnung Wählen Sie Drahtlosnetzwerke mit aktivierten Sicherheitsfunktionen

Wenn Sie die Verbindung zu einem Drahtlosnetzwerk herstellen, das nicht Ihr eigenes ist, sollten Sie immer ein Drahtlosnetzwerk mit aktivierten Sicherheitsfunktionen verwenden (sofern verfügbar). Falls Sie die Verbindung zu einem Netzwerk herstellen, das nicht geschützt ist, kann jemand mit den richtigen Tools alles sehen, was Sie tun: welche Websites Sie besuchen, welche Dokumente Sie bearbeiten und welche Benutzernamen und Kennwörter Sie eingeben – definitiv nicht zu empfehlen.

Wenn Sie bereits vorher Verbindungen zu mehreren Drahtlosnetzwerken hatten, wird die Liste dieser Netzwerke als Liste der bevorzugten Netzwerke bezeichnet. Die Drahtlosnetzwerke auf dieser Liste sind Ihre bevorzugten Drahtlosnetzwerke. Sie können im Netzwerk- und Freigabecenter auf *Drahtlosnetzwerke verwalten* klicken und sich die gespeicherten Drahtlosnetzwerke ansehen. Sie können die Reihenfolge ändern, in der Ihr Computer versucht, eine Verbindung zu den bevorzugten Netzwerken herzustellen. Dazu können Sie die Netzwerke in der Liste nach oben oder unten verschieben. Sie können auch die Voreinstellungen für das Netzwerk ändern, indem Sie mit der rechten Maustaste auf das Netzwerk klicken und den Befehl *Eigenschaften* wählen.

Nehmen wir an, eine Ärztin arbeitet in einem großen Krankenhaus. Im Erdgeschoss bekommt sie Verbindung zu den Drahtlosnetzwerken *Abteilungen_10_bis_14* und *Abteilungen_15_bis_19*. Im ersten Stock ist sie in Reichweite der Drahtlosnetzwerke *Abteilungen_20_bis_24* und *Abteilungen_25_bis_29*. Zwischen den Stockwerken ist eine Abschirmung, daher kann sie keine Verbindung zu einem Netzwerk im anderen Stockwerk herstellen. Sie weiß, dass die Netzwerke *Abteilungen_10_bis_14* und *Abteilungen_20_bis_24* eine hohe Bandbreite haben. Daher will sie nach Möglichkeit eine Verbindung zu einem dieser beiden Netzwerke herstellen, je nachdem, in welchem Stockwerk sie sich befindet. Ist es nicht möglich, eine Verbindung mit dem einen herzustellen, soll das andere verwendet werden.

Die Ärztin hat früher bereits mit allen vier Netzwerken Verbindung gehabt (aber nicht gleichzeitig), und sie stehen alle auf der Liste der bevorzugten Netzwerke. Beachten Sie, dass ein Netzwerk sogar dann auf der Liste der bevorzugten Netzwerke stehen kann, wenn es momentan nicht in Reichweite ist. Die Ärztin muss sicherstellen, dass das Netzwerk *Abteilungen_10_bis_14* in ihrer Liste der bevorzugten Netzwerke über *Abteilungen_15_bis_19* steht, und das Netzwerk *Abteilungen_20_bis_24* über *Abteilungen_25_bis_29*. Es ist egal, ob die Netzwerke des Erdgeschosses in der Liste über denen des ersten Stocks stehen oder umgekehrt.

Im Erdgeschoss sind die Netzwerke des ersten Stocks nicht erreichbar. Der Computer der Ärztin stellt daher eine Verbindung zum Netzwerk *Abteilungen_10_bis_14* her, sofern es in Reichweite ist. Falls nicht, baut er eine Verbindung zum Netzwerk *Abteilungen_15_bis_19* auf. Im ersten Stock sind wiederum die Netzwerke des Erdgeschosses nicht erreichbar. Der Computer der Ärztin baut also eine Verbindung zum Netzwerk *Abteilungen_20_bis_24* auf, wenn das möglich ist. Andernfalls verbindet er sich mit dem Netzwerk *Abteilungen_25_bis_29*.

Konfigurieren der Sicherheitseinstellungen für interne Drahtlosadapter

Weiter unten in dieser Lektion lernen Sie, wie Sie die Sicherheitseinstellungen im WAP eines anderen Herstellers konfigurieren. Sie müssen aber auch in einem Drahtlosnetzwerkadapter kompatible Sicherheitseinstellungen konfigurieren. In der Standardeinstellung ist ein WAP so eingerichtet, dass er allen drahtlosfähigen Computern, die sich in Reichweite befinden, den Zugriff erlaubt. Er kann aber so konfiguriert werden, dass er den Zugriff auf authentifizierte Verbindungen beschränkt und einen bestimmten Verschlüsselungsstandard einsetzt. Sie konfigurieren sowohl Authentifizierung als auch Verschlüsselung für einen Drahtlosnetzwerkadapter auf der Registerkarte *Sicherheit* im Dialogfeld *Eigenschaften für Drahtlosnetzwerk*. Abbildung 6.40 zeigt dieses Dialogfeld mit den verfügbaren Sicherheitstypen. Der Verschlüsselungstyp ist beim Sicherheitstyp *Keine Authentifizierung* entweder *Keine* oder *WEP* (Wired Equivalent Privacy).

Es stehen folgende Authentifizierungstypen zur Auswahl:

- *Keine Authentifizierung (Offen)*
- *Gemeinsam verwendet* (ein vorinstallierter Schlüssel)
- *WPA-Personal* (Wi-Fi Protected Access)
- *WPA2-Personal*
- *WPA-Enterprise*
- *WPA2-Enterprise*
- *802.1X*

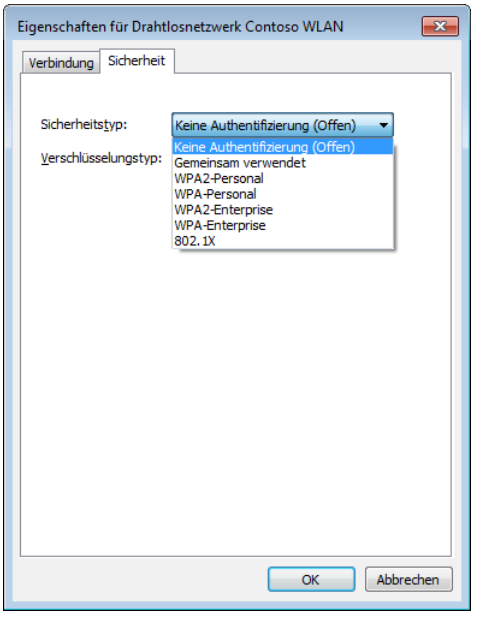


Abbildung 6.40 Die Registerkarte Sicherheit im Dialogfeld *Eigenschaften für Drahtlosnetzwerk*

WPA und WPA2 bieten Kompatibilität zu dem Sicherheitsprotokoll, das von der Wi-Fi Alliance zum Schutz von Drahtlosnetzwerken entwickelt wurde. WPA2 verbessert WPA, das seinerseits Schwachstellen im Vorgängersystem WEP beseitigt. WPA war als vorübergehender Ersatz für WEP gedacht, während der Standard IEEE 802.11i vorbereitet wurde. 802.1X bietet portbasierte Authentifizierung, bei der ein Anforderer (ein Clientcomputer), ein Authentifizierer (ein Ethernetkabelswitch oder WAP) und ein authentifizierender Server (meist ein RADIUS-Server) miteinander kommunizieren.

Die WPA2-Zertifizierung bietet Kompatibilität zu einem erweiterten Protokoll, das den Standard 802.11 vollständig implementiert. Es ist für alle neuen Drahtlosrouter obligatorisch, die das Wi-Fi-Markenzeichen tragen. Dieses erweiterte Protokoll funktioniert bei einigen alten Netzwerkkarten nicht, daher wird WPA in Microsoft-Betriebssystemen weiterhin unterstützt, auch in Windows 7. Der Hauptunterschied zwischen WPA und WPA2 ist, dass WPA2 mit AES (Advanced Encryption Standard) arbeitet. AES hat einen eigenen Mechanismus, um dynamische Schlüssel zu generieren, und ist widerstandsfähiger gegenüber einer statistischen Analyse des Ciphertextes.

Vorinstallierte Schlüssel (Pre-Shared Key, PSK) werden auch als *Personal*-Modi bezeichnet. Sie sind für SOHO-Netzwerke gedacht, in denen keine komplexe 802.1X-Authentifizierung benötigt wird und die keinen Zertifizierungsstellenserver enthalten. Jedes Drahtlosnetzwerkgerät verschlüsselt den Netzwerkverkehr dabei mit einem 256-Bit-Schlüssel. Dieser Schlüssel wird entweder als Zeichenfolge mit 64 Hexadezimalziffern oder als Passphrase mit 8 bis 63 druckbaren ASCII-Zeichen eingegeben. Windows 7 unterstützt die Modi *WPA-Personal* und *WPA2-Personal*.

WPA-Enterprise und *WPA2-Enterprise* führen die Authentifizierung mithilfe von EAP (Extensible Authentication Protocol) durch. Sie erfordern Computersicherheitszertifikate statt PSKs. Folgende EAP-Typen sind im Zertifizierungsprogramm enthalten:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM



Weitere Informationen EAP

Weitere Informationen über EAP finden Sie unter *http://technet.microsoft.com/en-us/network/bb643147.aspx*.

Der Authentifizierungstyp, den Sie für Ihre Netzwerkkarte konfigurieren, muss von den Netzwerken unterstützt werden, zu denen Sie über diese Netzwerkhardware eine Verbindung herstellen wollen. Das bedeutet beispielsweise:

- Wenn Sie einen RADIUS-Server in Ihrem Netzwerk haben, der als authentifizierender Server agiert, und Sie optimale Sicherheit brauchen, sollten Sie 802.1X wählen.
- Wenn Sie keinen PSK, sondern Computerzertifikate und AES verwenden wollen, sollten Sie WPA2-Enterprise wählen.
- Falls Ihr Netzwerkrouter AES nicht unterstützt, aber Sie Computerzertifikate verwenden wollen, sollten Sie WPA-Enterprise wählen.
- Wenn Sie ein kleines Netzwerk haben, das nicht in einer Domäne liegt und nicht auf einen Zertifizierungsstellenserver zugreifen kann, Sie aber einen modernen WAP installieren, der AES unterstützt, sollten Sie WPA2-Personal (mit einem PSK) verwenden.
- Wenn Sie ein kleines Netzwerk haben, das nicht in einer Domäne liegt und nicht auf einen Zertifizierungsstellenserver zugreifen kann, und Ihr WAP keine Unterstützung für AES bietet, sollten Sie WPA-Personal wählen.
- Der Sicherheitstyp *Gemeinsam verwendet* arbeitet mit einer vorinstallierten Passphrase, bietet aber keinen weiteren Schutz. Sie sollten diesen Typ nur wählen, wenn keine andere Methode möglich ist.
- In der Standardeinstellung führt ein unkonfigurierter WAP keine Authentifizierung durch. Ein solcher WAP ist ein Sicherheitsrisiko, daher ist es hochgradig fahrlässig und unprofessionell, ihn in diesem Zustand zu betreiben.

Ist keine Authentifizierung konfiguriert, kann jeder eine Verbindung zwischen seinem Computer und Ihrem Netzwerk herstellen. Wird keine Verschlüsselung durchgeführt, kann jemand mit einem Protokollsniffer vertrauliche Daten abfangen und lesen.



Weitere Informationen WEP und WPA

Weitere Informationen über WEP und WPA finden Sie unter *http://www.ezlan.net/wpa_wep.html*. Dies ist keine TechNet-Site, sie wird von einem Microsoft-MVP (Most Valued Professional) betrieben.

Verwenden eines Ad-hoc-Netzwerks

Sie können ein temporäres Drahtlosnetzwerk, ein sogenanntes Ad-hoc-Netzwerk, zwischen zwei oder mehr Windows 7-Computern (oder zwischen Computern mit Windows 7 und Windows Vista) einrichten, sofern sie nicht weiter als 10 Meter voneinander entfernt sind. Sie brauchen keinen WAP, um ein Ad-hoc-Netzwerk einzurichten. So können Benutzer Ordner und andere Ressourcen freigeben, ohne eine Verbindung zu einem Unternehmensnetzwerk herstellen zu müssen.

Nehmen wir an, Sie halten ein Meeting mit Vertretern anderer Unternehmen ab und wollen Informationen mit ihnen austauschen (etwa Produktspezifikationen), ohne ihnen allerdings Zugriff auf Ihr Unternehmensnetzwerk zu gewähren. Oder Sie haben ein Meeting in einem Hotelzimmer und wollen keine vertraulichen Informationen über das Netzwerk des Hotels leiten. In solchen Fällen können Sie ganz einfach und schnell ein Ad-hoc-Netzwerk einrichten. Wie das geht, erklären die folgenden Absätze.

Öffnen Sie auf dem ersten Computer im Netzwerk das Netzwerk- und Freigabecenter und klicken Sie auf *Neue Verbindung oder neues Netzwerk einrichten*. Wählen Sie die Option *Ein drahtloses Ad-hoc-Netzwerk (Computer-zu-Computer) einrichten* aus. Geben Sie dem Netzwerk einen Namen und legen Sie (bei Bedarf) einen Sicherheitsschlüssel fest, sodass Benutzer, die dem Netzwerk beitreten wollen, ein Kennwort angeben müssen. Bei WEP können dies 5 Zeichen sein, bei denen zwischen Groß- und Kleinschreibung unterschieden wird, 13 Zeichen mit Unterscheidung zwischen Groß- und Kleinschreibung, 10 Hexadezimalzeichen, bei denen nicht zwischen Groß- und Kleinschreibung unterschieden wird, oder 26 Hexadezimalzeichen ohne Unterscheidung zwischen Groß- und Kleinschreibung. Welche Möglichkeit Sie wählen, hängt von den Sicherheitsanforderungen ab. (Wenn Sie WPA2-Personal verwenden, können Sie auf einem 64 Zeichen langen Kennwort bestehen. Aber bis das von allen eingetippt wurde, ist das Meeting wahrscheinlich vorbei.)

Andere Benutzer treten dem Ad-hoc-Netzwerk genauso bei wie jedem anderen Drahtlosnetzwerk. Sie können auswählen, ob Sie die Netzwerkeinstellungen speichern wollen, für den Fall, dass Sie in Zukunft ein weiteres Ad-hoc-Netzwerk mit denselben Einstellungen einrichten wollen. Aber meist sind Ad-hoc-Netzwerke temporär und verschwinden, sobald das letzte Mitglied das Netzwerk verlässt. Ad-hoc-Netzwerke arbeiten mit IPv6 und benötigen keine IPv4-Konnektivität. In den Übungen weiter unten in dieser Lektion richten Sie ein Ad-hoc-Netzwerk ein und treten ihm bei.

Ad-hoc-Netzwerke sind beispielsweise nützlich, wenn Sie eine Verbindung ins Internet über ein internes Mobilfunkmodem oder ein UMTS-Telefon herstellen. Auf eine solche Verbindung können nicht mehrere Computer gleichzeitig zugreifen (anders als beim Internetzugriff über einen WAP und ein DSL-Modem). In diesem Fall können Sie ein Ad-hoc-Netzwerk einrichten und Ihre Internetverbindung über ICS freigeben, damit Freunde mit Drahtlosnotebooks auf das Internet zugreifen können, wenn sie zu Ihnen kommen.

Technologien für Drahtlosnetzwerke

Die Vorteile von Drahtlosnetzwerken sind Mobilität und einfache Hardwareinstallation (Sie brauchen keine Kabel zu verlegen). Nachteile sind eine (meist) langsamere Verbindung als beim Kabelnetzwerk und Störungen durch andere Drahtlosgeräte wie Funktelefone.

Derzeit sind vier Arten von Drahtlosnetzwerktechnologien weit verbreitet:

- **802.11b** Bis zu 11 Megabit pro Sekunde (MBit/s), hohe Signalreichweite, geringe Kosten. Diese Technologie erlaubt weniger gleichzeitige Benutzer als die anderen. Sie arbeitet im Frequenzbereich 2,4 GHz. Diese Frequenz ist oft Störungen durch Mikrowellenherde, Funktelefone und andere Haushaltsgeräte ausgesetzt.
- **802.11a** Bis zu 54 MBit/s, mehr gleichzeitige Benutzer als 802.11b, aber geringere Signalreichweite, teuer. Diese Option bietet hohe Übertragungsgeschwindigkeit und arbeitet im Frequenzbereich 5 GHz, wodurch weniger Störungen durch andere Geräte auftreten. Das Signal wird aber durch Wände und andere Hindernisse stark gedämpft. Außerdem ist diese Technologie nicht kompatibel zu 802.11b-Netzwerkkarten, -Routern und -Zugriffspunkten.
- **802.11g** Bis zu 54 MBit/s (unter optimalen Bedingungen), mehr gleichzeitige Benutzer als 802.11b, sehr hohe Signalreichweite, relativ robust gegenüber Dämpfung durch Hindernisse. Diese Technologie ist kompatibel zu 802.11b-Netzwerkkarten, -Routern und -Zugriffspunkten, arbeitet aber im Frequenzbereich 2,4 GHz und hat dieselben Störungsprobleme wie 802.11b. Sie ist teurer als 802.11b.
- **802.11n** Gerade erst aus der Draftphase. Mehrere Hersteller liefern aber schon lange Geräte, die dem Draft-Standard 802.11n entsprechen. Die meisten 802.11n-Geräte sind kompatibel zu 802.11b und 802.11g. 802.11n baut auf den älteren 802.11-Standards auf und fügt MIMO (Multiple-Input, Multiple-Output) hinzu, sodass mehrere Sende- und Empfangsantennen benutzt werden können, um die Systemleistung zu erhöhen.

802.11b reicht für die meisten Heim- und viele kleine Unternehmensnetze aus. Falls Ihr Netzwerk allerdings viele Streamingdaten (Videos oder Musik) transportiert oder Störungen ein großes Problem sind, können Sie 802.11a in Betracht ziehen. Falls Sie bereits 802.11b-Geräte in Ihrem Netzwerk haben, aber Hochgeschwindigkeitsübertragung zwischen bestimmten Netzwerkpunkten benötigen, könnte sich 802.11g eignen. Die meisten modernen WAPs auf dem Markt beherrschen heute 802.11g und 802.11n.

Falls Sie mehr als eine Drahtlosnetzwerkkarte in Ihrem Computer haben oder Ihr Adapter mehr als einen Standard nutzt, können Sie angeben, welchen Adapter oder Standard Sie für jede Netzwerkverbindung verwenden wollen.



Prüfungstipp

Neben 802.11a, 802.11b und 802.11g gibt es noch einige weitere 802.11-Standards. Die in dieser Lektion beschriebenen Standards sind allerdings am weitesten verbreitet. Falls in der Antwort einer Prüfungsfrage ein anderer Standard erwähnt wird (zum Beispiel 802.11d), ist diese Antwort mit großer Wahrscheinlichkeit falsch.

Verwalten von Netzwerkverbindungen

Sie können sich eine Liste aller Verbindungsschnittstellen (Kabel oder drahtlos) auf einem Computer ansehen, indem Sie das Netzwerk- und Freigabecenter öffnen und auf *Adaptereinstellungen ändern* klicken. Klicken Sie mit der rechten Maustaste auf eine Netzwerkverbindung und wählen Sie den Befehl *Status*. Wenn Sie im Dialogfeld *Status von LAN-Verbindung* auf *Details* klicken, öffnet sich das Dialogfeld *Netzwerkverbindungsdetails* (siehe Abbildung 6.38 weiter oben in dieser Lektion).

Wenn in einem kleinen kabelgebundenen Heimnetzwerk ICS aktiviert ist, hat eine Arbeitsstation normalerweise eine Adresse im Netzwerk 192.168.0.0/24, dessen Standardgateway die Adresse 192.168.0.1 hat. Ein WAP ist normalerweise nicht mit der Adresse 192.168.0.1 konfiguriert, sondern hat oft eine IP-Adresse wie 192.168.123.254. Wie auch immer die Einstellungen in Ihrem Netzwerk lauten: Sie sollten sich die Konfiguration notieren, während alles einwandfrei läuft. Diese Informationen sind von unschätzbarem Wert, wenn etwas schiefgeht.



Hinweis Ändern der Netzwerkeinstellungen

Statt die ICS-Standardeinstellungen zu verwenden, ändern viele Administratoren sie gerne. Beispielsweise verwenden sie das Netzwerk 10.0.10.0/24 für kabelgebundene Computer und das Subnetz 192.168.123.0/24 für Drahtloscomputer. In der Prüfung 70-680 wird das Ändern der ICS-Standardeinstellungen allerdings nicht behandelt.

Wenn Sie mit der rechten Maustaste auf einen Adapter klicken und den Befehl *Eigenschaften* wählen, wird das Dialogfeld *Eigenschaften von LAN-Verbindung* geöffnet. In diesem Dialogfeld können Sie die angezeigten Elemente aktivieren oder deaktivieren und weitere Elemente installieren (Clientdienste, Serverdienste oder Protokolle), indem Sie auf *Installieren* klicken.

Normalerweise enthält das Dialogfeld *Eigenschaften von LAN-Verbindung* (gleichermaßen bei Kabel- wie auch Drahtlosverbindungen) die folgenden Elemente:

- **Client für Microsoft-Netzwerke** Ermöglicht es dem Computer, auf Ressourcen in einem Microsoft-Netzwerk zuzugreifen.
- **QoS-Paketplaner** Stellt Steuerungsmöglichkeiten für den Datenverkehr bereit. Das kann wichtig sein, wenn Sie in Ihrem Netzwerk Verkehr mit hoher Bandbreite übertragen, zum Beispiel Videostreaming.
- **Datei- und Druckerfreigabe für Microsoft-Netzwerke** Ermöglicht es anderen Computern in einem Microsoft-Netzwerk (und anderen Netzwerken), auf Ressourcen Ihres Computers zuzugreifen.
- **Internetprotokoll Version 6 (TCP/IPv6)** Hier haben Sie Zugriff auf die IPv6-Konfiguration.
- **Internetprotokoll Version 4 (TCP/IPv4)** Hier haben Sie Zugriff auf die IPv4-Konfiguration.
- **E/A-Treiber für Verbindungsschicht-Topologieerkennungszuordnung** Erkennt und sucht andere Computer, Geräte und Netzwerkinfrastrukturkomponenten im Netzwerk und ermittelt die Netzwerkbandbreite.

- **Antwort für Verbindungsschicht-Topologieerkennung** Ermöglicht es, dass der Computer im Netzwerk erkannt und gesucht werden kann.

Falls ein Element konfigurierbar ist, wird beim Auswählen des Elements die Schaltfläche *Eigenschaften* aktiviert. Wenn Sie diese Schaltfläche anklicken, können Sie die Eigenschaften des jeweiligen Elements konfigurieren. Sie können auch den Adapter selbst konfigurieren (zum Beispiel den Treiber aktualisieren), indem Sie im Dialogfeld *Eigenschaften von LAN-Verbindung* auf *Konfigurieren* klicken.

Notieren Sie sich, welche Elemente installiert und aktiviert sind, während die Netzwerkverbindungen Ihres Computers einwandfrei funktionieren. Wahrscheinlich haben alle anderen Computer in einem Netzwerk, das Sie verwalten, ähnliche Einstellungen (abgesehen von ihren IP-Adressen). Es empfiehlt sich aber, diesen Punkt zu überprüfen, zum Beispiel mithilfe des Remotedesktops. Diese Einstellungen brauchen Sie wahrscheinlich nur sehr selten zu ändern, aber falls etwas schiefgeht, können Sie herausfinden, welches die ursprünglichen Einstellungen waren.

Schnelltest

- In welchem Dialogfeld können Sie neue Protokolle, Serverdienste oder Clientdienste hinzufügen?

Antwort zum Schnelltest

- Im Dialogfeld *Eigenschaften von LAN-Verbindung*

Sie können auch im Dialogfeld *Netzwerkverbindungen* mit der rechten Maustaste auf eine Verbindung klicken und den Befehl *Diagnose* wählen. Daraufhin wird die Windows-Netzwerkdiagnose gestartet, wie in Lektion 1 dieses Kapitels beschrieben.

Falls Sie mehrere Netzwerkverbindungen haben, können Sie eine Netzwerkbrücke (bridge) erstellen, indem Sie zwei oder mehr Verbindungen auswählen (klicken Sie alle gewünschten Verbindungen an, während Sie die STRG-Taste gedrückt halten), mit der rechten Maustaste klicken und den Befehl *Verbindungen überbrücken* wählen. Wenn Sie nicht als Administrator angemeldet sind, werden Sie aufgefordert, entsprechende Anmeldeinformationen einzugeben.

Eine Netzwerkbrücke ist Software oder Hardware, die zwei oder mehr Netzwerke verbindet, sodass sie miteinander kommunizieren können. Wenn Sie ein Netzwerk verwalten, das unterschiedliche Netzwerktypen umfasst (etwa ein Kabel- und ein Drahtlosnetzwerk), verwenden Sie gewöhnlich eine Brücke, wenn Sie zwischen allen Computern in diesen Netzwerken Informationen austauschen oder Dateien freigeben wollen. Wenn Sie die Netzwerkbrückensoftware verwenden, die in Windows 7 integriert ist, benötigen Sie keine zusätzliche Hardware.

Problembehandlung für Drahtlosnetzwerke

Lektion 1 hat die grundlegende Problembehandlung beschrieben und erklärt, wie Sie Konnektivitätsprobleme beseitigen. Es gibt allerdings einige Verbindungsprobleme, die speziell bei Drahtlosnetzwerken auftreten. Sie müssen ihre Ursachen kennen und wissen, wie Sie sie beseitigen.

Verhindern, dass Ihr Computer zwischen WAPs umschaltet

Wenn Sie oder Benutzer, für die Sie Support leisten, sich mit einem mobilen drahtlosfähigen Computer bewegen, schaltet der Computer von einem Drahtlosnetzwerk zum nächsten, um eine Verbindung aufrechtzuerhalten. Das ist normal, wenn die automatische Umschaltung aktiviert ist. Sie wird beispielsweise in größeren Firmen, Krankenhäusern oder Universitäten eingesetzt, die so groß sind, dass sie nicht mit einem einzigen Netzwerk abgedeckt werden können.

Es können aber Probleme auftreten, wenn ein Ort von mehreren Drahtlosnetzwerken abgedeckt wird und ein Computer versucht, zwischen diesen Zugriffspunkten umzuschalten, obwohl der Benutzer seine Position gar nicht ändert. Das kann dazu führen, dass die Verbindung des Benutzers zeitweise unterbrochen wird oder der Computer die Verbindung ganz verliert.

Bei 802.11b- und 802.11g-Routern und -Zugriffspunkten beträgt die maximale Reichweite etwa 50 Meter in Räumen und etwa 100 Meter im Freien. Bei 802.11a-Routern und -Zugriffspunkten beträgt die maximale Reichweite etwa 15 Meter in Räumen und 30 Meter im Freien. Diese Reichweiten gelten unter optimalen Bedingungen ohne Störeinflüsse. Wenn ein drahtlosfähiger Computer beispielsweise ein Desktopcomputer ist, der 15 Meter vom ersten WAP und 20 Meter von einem zweiten WAP entfernt ist, können Probleme auftreten. Sie können den Benutzer bitten, den Computer woanders hinzustellen (normalerweise nicht praktikabel) oder die automatische Umschaltung bei einem oder beiden Netzwerkprofilen auszuschalten.

Dazu deaktivieren Sie das Kontrollkästchen *Mit einem verfügbaren bevorzugten Netzwerk verbinden* im Dialogfeld *Eigenschaften für Drahtlosnetzwerk* (siehe Abbildung 6.39 weiter oben in dieser Lektion). Dabei steht es Ihnen frei, welches der beiden überlappenden Netzwerke Sie deaktivieren. Anschließend muss der Benutzer von Hand das Netzwerk suchen und eine Verbindung dazu herstellen, wenn er es verwenden will. Der Computer versucht nicht mehr, Verbindungen zu beiden Netzwerken aufzubauen.



Warnung Das Deaktivieren der automatischen Umschaltung ist nicht immer sinnvoll

Sie können die automatische Umschaltung zwischen bevorzugten Netzwerken deaktivieren, um die Probleme zu beseitigen, die auftreten, wenn ein Benutzer in einem Überlappungsbereich arbeitet. Dabei müssen Sie aber natürlich sehr aufpassen. Eine Ärztin, die in einem Krankenhaus arbeitet, will nicht von Hand die Verbindung zu einem anderen WAP herstellen, wenn sie sich von einer Abteilung zu einer anderen bewegt. Ein Lehrer will nicht seine Einstellungen anpassen, wenn er zur nächsten Klasse geht. Stellen Sie immer sicher, dass Ihren Benutzern die Nachteile dieser »Reparatur« klar sind.

Verringern von Störungen

Um Störungen durch Geräte wie Mobiltelefone und Mikrowellenherde zu verringern, können Sie den von Ihrem WAP benutzten Kanal wechseln. Manche Kanäle sind weniger störanfällig als andere. Wie Sie den WAP eines bestimmten Herstellers konfigurieren, ist im Handbuch des Geräts beschrieben. Sie können die meisten WAPs über eine Weboberfläche von einem beliebigen Computer im Netzwerk aus einrichten.

Hat ein WAP beispielsweise die IPv4-Adresse 192.168.123.154, geben Sie im Browser die Adresse **http://192.168.123.254** ein. Daraufhin öffnet sich eine Konfigurationsseite, die zum

Beispiel wie in Abbildung 6.41 aussieht. Dies ist die Setupseite für einen beliebigen WAP mit Standardeinstellungen. Auch wenn die entsprechende Bedienoberfläche in Ihrem Netzwerk wahrscheinlich anders aussieht, können Sie sich meistens anmelden und die Kanaleinstellungen ändern. Es hängt von mehreren Faktoren ab, auf welchem Kanal Sie die geringsten Störungen haben, darunter Aufstellungsort und Typ der Geräte, die Störungen verursachen. Experimentieren Sie mit den Kanaleinstellungen, bis Sie die besten gefunden haben.

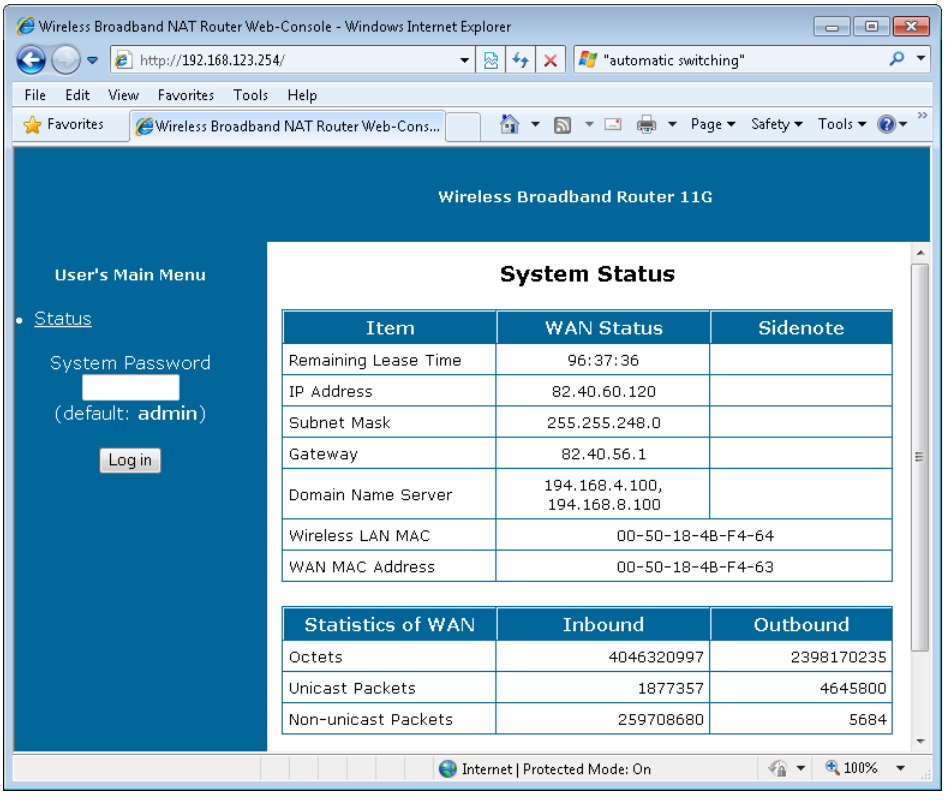


Abbildung 6.41 Die Konfigurationsoberfläche eines typischen WAPs

802.11b und 802.11g arbeiten im Frequenzbereich 2,4 GHz. Mikrowellenherde und Funktelefone verwenden ebenfalls diese Frequenz. 802.11a arbeitet im Frequenzbereich 5 GHz. Einige Funktelefone verwenden ebenfalls diese Frequenz. Falls diese Geräte Störungen zwischen einem Computer und dem Netzwerk verursachen, mit dem er verbunden ist, versucht der Computer unter Umständen, zu einem anderen benachbarten Netzwerk umzuschalten. Es ist kaum praktikabel, dass Sie Ihre Familie bitten, nicht zu telefonieren, und Ihre Nachbarn auffordern, mit dem Aufwärmen ihres Essens in der Mikrowelle zu warten, während Sie im Internet surfen. Die Lösung besteht darin, die WAP-Einstellungen so zu ändern, dass ein anderer Funkkanal verwendet wird. Sie können auch einstellen, dass der Kanal automatisch ausgewählt wird, falls bisher eine feste Kanalnummer konfiguriert ist. In Europa können Sie die Kanäle 1 bis 13 verwenden. Das Handbuch zu Ihrem WAP müsste beschreiben, wie Sie den Funkkanal einstellen.

Netzwerke mit derselben SSID

Die SSID (Service Set Identifier) ist die Kennung Ihres Drahtlosnetzwerks. Hat ein Netzwerk in Ihrer Liste der bevorzugten Drahtlosnetzwerke dieselbe SSID wie ein anderes Netzwerk, das sich in der Reichweite Ihres Computers befindet, versucht Windows unter Umständen, zwischen den beiden WAPs umzuschalten, weil es sie als dasselbe Netzwerk ansieht. Normalerweise lautet die Standard-SSID eines WAP »Default«. Wenn mehrere Leute Drahtlosnetzwerke einrichten, zum Beispiel in einem Wohnhaus oder in einem Büroblock mit mehreren kleinen Firmen, und niemand die Standardeinstellung ändert, können Probleme auftreten. In diesem Fall besteht die Lösung darin, jedem WAP eine eindeutige SSID zu geben.

Abbildung 6.42 zeigt die Setupseite eines WAP, dessen Standardeinstellungen noch nicht verändert wurden. Auf dieser Seite können Sie den Kanal und die SSID ändern.

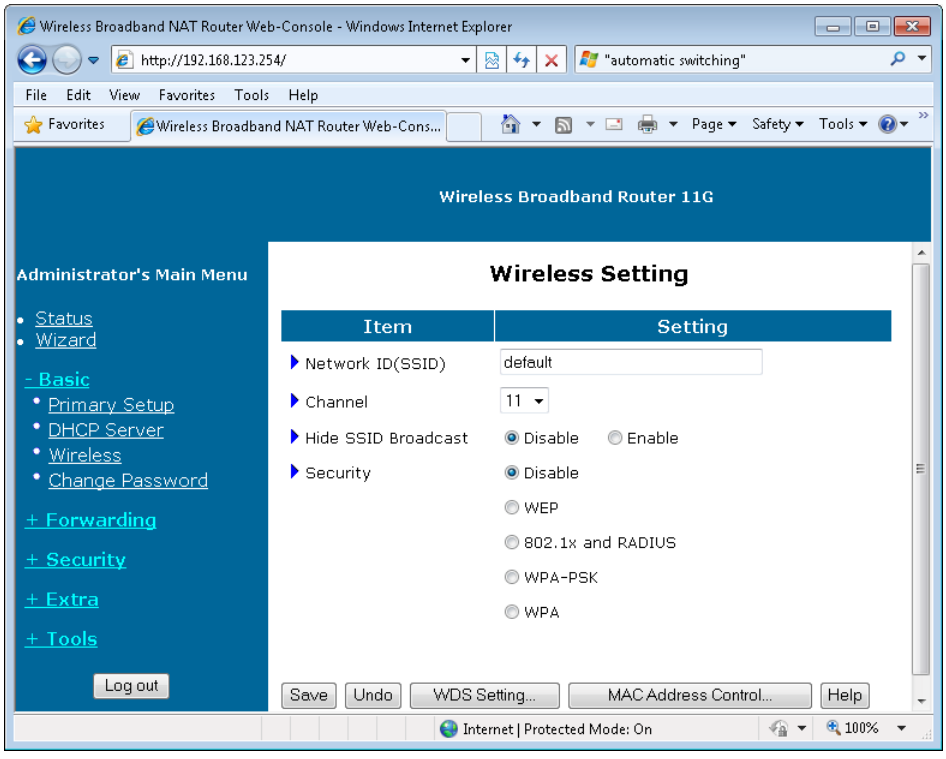


Abbildung 6.42 SSID-, Kanal-, SSID-Broadcast- und Sicherheitseinstellungen bei einem typischen WAP

Sie sollten ein Drahtlosnetzwerk immer schützen, indem Sie die SSID ändern und andere Sicherheitseinstellungen wählen, wie weiter unten in dieser Lektion beschrieben. Wenn Sie Ihr Drahtlosnetzwerk nicht absichern, braucht ein Dieb nicht einmal mehr bei Ihnen einzubrechen. Er kann in seinem Auto vor Ihrem Haus sitzen, sein WLAN-fähiges Notebook einschalten, Ihre Kennwörter ausspähen und Ihr Bankkonto abräumen. Falls Sie ein Drahtlosnetzwerk für Ihr Unternehmen einrichten, ohne es zu schützen, könnte es sein, dass Ihr Unternehmen bald pleite geht und Sie sich auf dem Arbeitsamt wiederfinden.

Praxistipp

Ian McLean

Ein Freund von mir arbeitete in der Kundensupportabteilung eines Computerhändlers. Vor einiger Zeit, als Drahtlosnetzwerke im Heimbereich noch recht selten waren, bekam er am selben Tag drei Anrufe von Kunden, die Probleme mit Verzögerungen und Verbindungsabbrüchen bei ihren Drahtlosnetzwerken hatten. In einem Fall hatte das Netzwerk eine Woche lang einwandfrei funktioniert, bevor die Probleme begannen. In den beiden anderen Fällen waren die Netzwerke gerade neu installiert worden.

Mein Freund überprüfte die Adressen dieser Kunden. Sie waren Nachbarn. Offensichtlich hatte einer von ihnen ein Drahtlosnetzwerk eingerichtet und war so begeistert davon, dass er es stolz seinen Nachbarn vorführte. Sie waren angesteckt von der Begeisterung und kauften genau dieselben Modelle, mit genau denselben Voreinstellungen.

Konfigurieren der Sicherheit für Drahtlosnetzwerke

Viele Verbindungsprobleme bei Drahtlosnetzwerken haben mit der Sicherheit zu tun. Welche konkreten Schritte erforderlich sind, um die Sicherheitseinstellungen vorzunehmen, hängt vom Typ des WAP ab, den Sie in Ihrem Netzwerk installiert haben. Dieser Abschnitt beschreibt die Einstellungen, die in den meisten WAPs zur Verfügung stehen, und erklärt, wie Sie die Sicherheit in Drahtlosnetzwerken verbessern können. Sie können die folgenden Schritte durchführen, um die Sicherheit in Ihrem Drahtlosnetzwerk zu erhöhen:

- **Ändern der Standard-SSID** Das machen Sie normalerweise, damit benachbarte Netzwerke mit Standardeinstellungen keine Konflikte mit Ihrem Drahtlosnetzwerk verursachen. Das Ändern einer SSID verbessert die Netzwerksicherheit, weil Hacker, die ein Netzwerk mit Standard-SSID sehen, messerscharf schließen, dass es sich um ein schlecht konfiguriertes Netzwerk handelt, bei dem sich ein Angriff eher lohnt.
- **Einschalten der WPA- oder WEP-Verschlüsselung** Alle WLAN-Geräte unterstützen irgendeine Form der Verschlüsselung, die alle über Funknetzwerke gesendeten Nachrichten schützt, sodass sie nicht ohne Weiteres gelesen werden können, selbst wenn sie abgehört werden. Sie sollten die stärkste Verschlüsselung wählen, die in Ihrem Drahtlosnetzwerk zur Verfügung steht. Es müssen aber alle Drahtlosgeräte in Ihrem LAN dieselben Verschlüsselungseinstellungen verwenden. Daher müssen Sie die sicherste Einstellung finden, die Sie sowohl auf Ihrem WAP als auch Ihren Drahtlosadaptern konfigurieren können. Sie konfigurieren die Authentifizierungs- und Verschlüsselungseinstellungen für Ihre Drahtlosadapter auf der Registerkarte *Sicherheit* des Dialogfelds *Eigenschaften für Drahtlosnetzwerk*, wie weiter oben in dieser Lektion beschrieben.
- **Ändern der Standard-Administratorkennwörter** Die Webseitenoberfläche, auf der Sie den WAP eines Fremdherstellers konfigurieren, zeigt normalerweise ein Anmeldedialogfeld an, in dem Sie zumindest ein Kennwort (oft »admin«) und manchmal einen Benutzernamen eingeben müssen. Die Standardeinstellungen sind bei Hackern wohlbekannt. Ändern Sie sie.
- **Aktivieren der MAC-Adressfilterung** Dies wird als relativ komplexe Konfiguration betrachtet, weil MAC-Adressen (48 Bit lange Hexadezimalzahlen) recht kompliziert aussehen. Viele Administratoren denken, sie müssten alle ihre Netzwerkgeräte

abklappern, jeweils den Befehl `ipconfig /all` eingeben, die MAC-Adressen notieren und diese Informationen dann in der WAP-Konfigurationswebseite eingeben. Diese zeitraubende Prozedur ist aber gar nicht nötig. ARP löst IP-Adressen in MAC-Adressen auf und speichert die Ergebnisse in einem Cache. Sie brauchen sich also lediglich an einen einzigen Computer in Ihrem Netzwerk zu setzen, alle Netzwerkgeräte anzupingen (sofern die Firewalls das erlauben) und dann den Inhalt des ARP-Caches in eine Textdatei zu kopieren, deren Inhalt Sie in die WAP-Konfigurationsoberfläche übertragen. Sofern es nicht erforderlich ist, dass andere Notebooks Ihr Drahtlosnetzwerk benutzen (etwa in einem Hotel), sollten Sie die MAC-Filterung konfigurieren, um Ihr Netzwerk zu schützen.

- **Deaktivieren von SSID-Broadcast** Ein WAP sendet seine SSID normalerweise in regelmäßigen Abständen aus. Dieses Feature wurde für Unternehmen und WLAN-Hotspots entwickelt, wo ständig Drahtlosclients kommen und gehen. In einem Heimnetzwerk und vielen kleinen Büronetzwerken ist dieses Feature überflüssig und vergrößert die Gefahr, dass ein Hacker versucht, sich anzumelden. Wenn Sie die Einstellungen Ihres WAP kennen, können Sie die Verbindung dazu entweder im Netzwerk- und Freigabecenter oder mit einem Netsh-Befehl herstellen, wie weiter oben in dieser Lektion beschrieben.
- **Keine automatische Verbindung zu offenen Drahtlosnetzwerken herstellen** Wenn Sie eine automatische Verbindung zu einem ungeschützten Drahtlosnetzwerk aufbauen, setzen Sie einen Computer damit Gefahren aus. Manche Netzwerkkarten haben eine Einstellung, die das verhindert. Dies ist eine spezielle Einstellung des jeweiligen Adapters, nicht von Windows 7. Ist allerdings Windows Live One-Care installiert, verbessert es die Browser- und Firewallsicherheit, falls ein Computer doch eine Verbindung zu einem ungeschützten Netzwerk aufbaut.
- **Aktivieren von Firewalls** Stellen Sie sicher, dass die Windows-Firewall auf WLAN-Computern aktiviert ist. Falls der WAP eine eingebaute Firewall hat, sollten Sie überprüfen, ob auch diese Firewall aktiviert ist.
- **Stellen Sie den WAP an einer zentralen Stelle auf** Funksignale reichen normalerweise über eine Wohnung oder ein Büro hinaus, aber Sie sollten die Reichweite nach außen so weit wie möglich verringern. Stellen Sie den WAP möglichst in der Mitte des Gebäudes auf, also nicht aufs Fensterbrett.
- **Ausschalten des Netzwerks, wenn es länger nicht benutzt wird** Es ist vielleicht unpraktisch, einen WAP häufig auszuschalten, aber wenn das Netzwerk längere Zeit nicht benutzt wird (beispielsweise während der Betriebsferien oder über mehrere Feiertage hinweg), sollten Sie das in Erwägung ziehen.
- **Zuweisen statischer IP-Adressen an Drahtlosclients** DHCP macht die Konfiguration einfach und verhältnismäßig fehlerfrei. Wenn allerdings jemand versucht, das Netzwerk anzugreifen, kann er gültige IP-Adressen aus dem DHCP-Pool des Netzwerks erhalten. Bei den meisten WAPs können Sie DHCP deaktivieren. Dann weisen Sie all Ihren Netzwerkgeräten private statische IP-Adressen zu. Das verbessert die Sicherheit, aber die statische Konfiguration ist unbequem und fehlerträchtig. Sie sollten diese Möglichkeit nur in Netzwerken in Betracht ziehen, wo Sicherheit von ganz entscheidender Bedeutung ist, oder in Netzwerken, wo Ihr WAP zum Beispiel Probleme hat, externe DNS-Einstellungen über DHCP zu konfigurieren.

Verbesserungen beim Drucken in Windows 7

Windows 7 führt standortabhängiges Drucken, Druckertreiberisolation, konfigurierbare Standardsicherheitseinstellungen für den Spooler und eine verbesserte Point-and-Print-Oberfläche für die Benutzer ein. Diese Verbesserungen bauen auf Features auf, die in Windows Vista eingeführt wurden und in Windows 7 weiterhin vollständig unterstützt werden, beispielsweise hochauflösende Druckausgabe, bessere Druckleistung, einfachere Verwaltung von Druckern und Druckservern, integrierte Unterstützung für das neue XPS (XML Paper Specification) und das Windows Color System.

Auf einem Windows 7-Computer profitieren Sie von der integrierten Unterstützung für das neue XPS (XML Paper Specification), das Inhalt und Aussehen von Druckdokumenten beschreibt. Die Dokumentdruckfunktionen von XPS unterstützen Vektorgrafik, die in einem weiten Bereich skaliert werden kann, ohne dass kantiger oder verpixelter Text entsteht. Ein XPS-Dokument wird standardmäßig generiert, wenn Sie in irgendeiner Anwendung unter Windows 7 drucken. Dieses Dokument können Sie mithilfe des Microsoft XPS-Dokument-Generators auf einem XPS-fähigen Drucker ausgeben, ohne dass es neu gerendert werden muss. Mithilfe des Microsoft XPS-Viewers können Sie sich XPS-Dokumente im Internet Explorer ansehen.

In der Standardeinstellung rendert Windows 7 Druckaufträge auf dem Client, nicht auf dem Druckserver. Das kann die Druckverarbeitung deutlich beschleunigen, wenn für die Ausgabe XPS-fähige Drucker eingesetzt werden. Clientseitiges Rendering (Client-Side Rendering, CSR) funktioniert auch bei Nicht-XPS-Druckern, es entlastet CPU und Arbeitsspeicher auf Druckservern und verringert den Netzwerkverkehr. XPS-Dokumente rendern ein Bild nur ein einziges Mal, danach wird das gerenderte Bild auf weiteren Seiten des Druckauftrags wiederverwendet.

Das MMC-Snap-In *Druckverwaltung* wurde verbessert, sodass Administratoren darin nun Standardsicherheitseinstellungen für Druckserver und die Druckertreiberisolation konfigurieren können. Auch die benutzerdefinierten Filter wurden durch neue Filterkriterien erweitert, die eine leistungsfähigere Filterung erlauben.

Der Netzwerkdruckerinstallations-Assistent ist einfacher zu bedienen als der Assistent *Drucker hinzufügen* (der in Windows 7 weiterhin zur Verfügung steht) und bietet neue Fähigkeiten, die es für Benutzer einfacher machen, eine Verbindung zu Remotedruckern und lokalen Druckern herzustellen, die nicht Plug & Play-fähig sind. Standardbenutzer können Drucker installieren, sie brauchen dafür keine Administratorprivilegien.

Verbesserte Farbverwaltung

Das neue Windows Color System (WCS) verbessert den Farbdruck und unterstützt Drucker mit erweitertem Farbraum (Tintenstrahldrucker, die mehr als vier Farbtinten verwenden). Gehen Sie folgendermaßen vor, um die Druckqualität bei einem installierten Drucker zu verbessern:

1. Klicken Sie im Startmenü auf *Geräte und Drucker*.
2. Klicken Sie doppelt auf einen Drucker. Sie bekommen angezeigt, was für ein Drucker es ist. Sie können Namen, Sicherheitseinstellungen und andere Eigenschaften des Druckers ändern und Farb-, Layout- und Papiereinstellungen konfigurieren.
3. Klicken Sie doppelt auf *Druckoptionen anpassen*. Im Eigenschaftendialogfeld des Druckers (Abbildung 6.43) können Sie Farbeinstellungen und die Druckqualität sowie

den Graustufendruck konfigurieren. Mit weiteren Steuerelementen können Sie Duplexdruck (sofern verfügbar) einstellen, ein Wasserzeichen festlegen, Seiteneinstellungen wählen und Geräteoptionen konfigurieren.

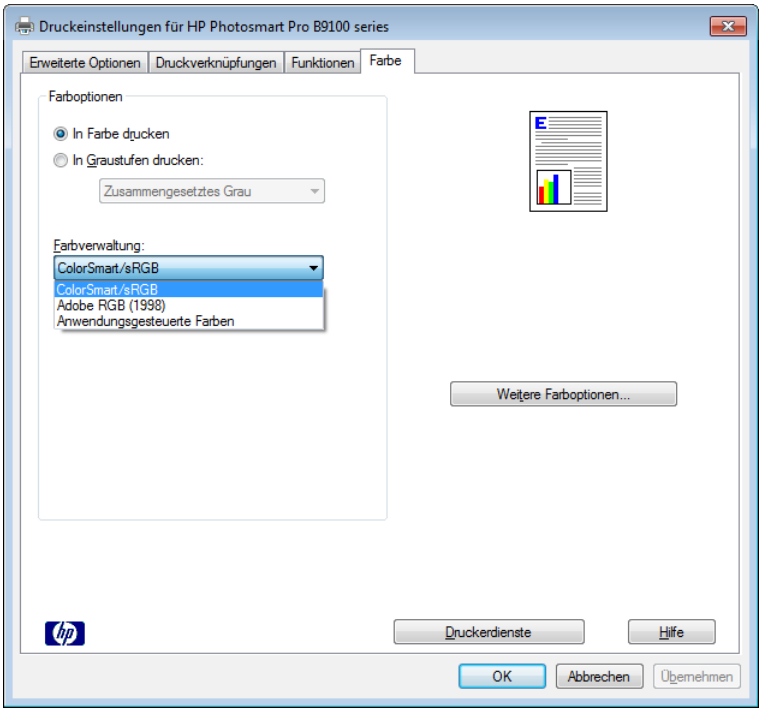


Abbildung 6.43 Das Eigenschaftendialogfeld eines Druckers

Standortabhängiges Drucken

In Windows Vista konnten Sie Drucker anhand ihres Aufstellungsorts zuweisen. Dazu verwenden Sie Gruppenrichtlinien und verknüpfen Gruppenrichtlinienobjekte mit Standorten in den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS). Wenn sich mobile Benutzer an einen anderen Standort bewegen, werden die Gruppenrichtlinien für ihre Druckerverbindungen am neuen Ort aktualisiert. Und sobald ein Benutzer wieder an seinen normalen Arbeitsplatz zurückkehrt, werden die normalen Standarddrucker wiederhergestellt.

Windows 7 baut dieses Konzept aus und führt das standortabhängige Drucken ein. Dabei können die Benutzer mobiler Computer (beispielsweise Notebooks) für jeden konfigurierten Netzwerkstandort einen anderen Standarddrucker festlegen. Beachten Sie aber, dass standortabhängiges Drucken etwas anderes ist als die Zuweisung von Druckern anhand des AD DS-Standorts.

Microsoft hat das standortabhängige Drucken eingeführt, weil in Unternehmen immer mehr mobile Computer zum Einsatz kommen. Hier ein typisches Szenario:

- Don Hall, Angestellter der Firma A. Datum, bekommt vom Unternehmen ein Notebook, damit er im Büro und zu Hause arbeiten kann. Während er im Büro ist, stellt er mit dem Assistenten *Drucker hinzufügen* die Verbindung zu einem Laserdrucker her.

Der Drucker wird automatisch als Standarddrucker für das Unternehmensnetzwerk festgelegt.

- Als Don nach Hause kommt, fügt er einen Plug & Play-fähigen USB-Tintenstrahldrucker hinzu. Dieser Drucker wird automatisch als Standarddrucker für sein Heimnetzwerk eingetragen. Sobald Don am nächsten Tag wieder ins Büro geht und die Verbindung zum Unternehmensnetzwerk herstellt, wird wieder der Laserdrucker des Unternehmens zum Standarddrucker. Sobald er zu Hause wieder eine Verbindung zu seinem Heimnetzwerk hergestellt und den Tintenstrahldrucker angeschlossen hat, ist wiederum der Tintenstrahldrucker der Standarddrucker.
- Immer, wenn Don sich im Büro befindet, ist der Laserdrucker des Unternehmens sein Standarddrucker. Und während er zu Hause ist, ist sein privater Tintenstrahldrucker der Standarddrucker. Im Unterschied zu älteren Windows-Versionen braucht Don nicht jedes Mal, wenn er das Netzwerk wechselt, einen neuen Standarddrucker festlegen. Er braucht überhaupt nichts einzurichten oder zu konfigurieren, wenn er von einem Netzwerk zum anderen wechselt.

Wenn das standortabhängige Drucken auf einem Windows 7-Computer verfügbar ist, wird in der Symbolleiste des Fensters *Geräte und Drucker* die zusätzliche Schaltfläche *Standarddrucker verwalten* angezeigt. Wenn Sie diese Schaltfläche anklicken, öffnet sich das Dialogfeld *Standarddrucker verwalten* (Abbildung 6.44), in dem Sie den Standarddrucker für jedes verbundene Netzwerk konfigurieren können.

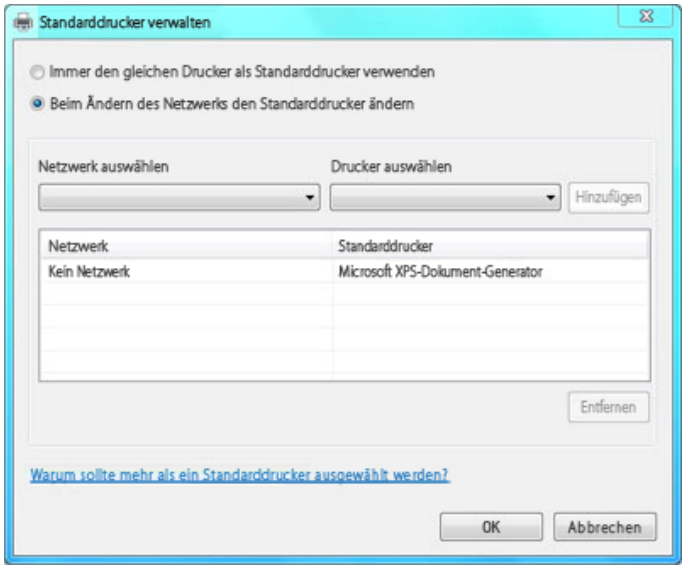


Abbildung 6.44 Das Dialogfeld *Standarddrucker verwalten*

Ist die Option *Beim Ändern des Netzwerks den Standarddrucker ändern* ausgewählt, können Sie in der Dropdownliste *Netzwerk auswählen* das gewünschte Netzwerk wählen. In der Dropdownliste *Drucker auswählen* wählen Sie den gewünschten Standarddrucker für das Netzwerk aus. Wenn ein Benutzer einen Drucker in einem Netzwerk installiert und ihn zum Standarddrucker macht, werden diese Einstellungen automatisch im Dialogfeld *Standarddrucker verwalten* konfiguriert. Sie können das standortabhängige Drucken deaktivieren,

indem Sie im Dialogfeld *Standarddrucker verwalten* die Option *Immer den gleichen Drucker als Standarddrucker verwenden* auswählen.

Übung Erstellen eines Ad-hoc-Netzwerks

In dieser Übung erstellen Sie ein Ad-hoc-Netzwerk, mit dem Sie die Computer *Aberdeen* und *Canberra* verbinden. Dafür müssen beide Computer Drahtlosadapter haben, weswegen dies eine optionale Übung ist.

Übung Erstellen eines Ad-hoc-Netzwerks

In dieser Übung erstellen Sie ein Ad-hoc-Netzwerk, während Sie unter dem Administratorkonto *Kim_Akers* am Computer *Aberdeen* angemeldet sind. Dann melden Sie sich mit einem Standardbenutzerkonto (kein Administrator) am Computer *Canberra* an und treten dem Ad-hoc-Netzwerk bei. Standardkonten haben Sie schon in den vorigen Übungen angelegt, beispielsweise das Konto *Don Hall* in Kapitel 4. Ist noch kein Standardkonto auf *Canberra* vorhanden, müssen Sie eines anlegen, bevor Sie die Übung beginnen.

Gehen Sie folgendermaßen vor, um ein Ad-hoc-Netzwerk zu erstellen:

1. Trennen Sie die Ethernetverbindung zwischen den beiden Computern und stellen Sie sicher, dass bei beiden Computern der Drahtlosadapter eingeschaltet ist.
2. Melden Sie sich mit dem Konto *Kim_Akers* am Computer *Aberdeen* an.
3. Legen Sie auf dem Computer *Aberdeen* einen Ordner namens *Test* an.
4. Klicken Sie mit der rechten Maustaste auf den Ordner *Test* und wählen Sie den Befehl *Eigenschaften*.
5. Klicken Sie auf der Registerkarte *Freigabe* auf *Erweiterte Freigabe* und geben Sie den Ordner so frei, dass die Gruppe *Jeder* Leseberechtigungen hat.

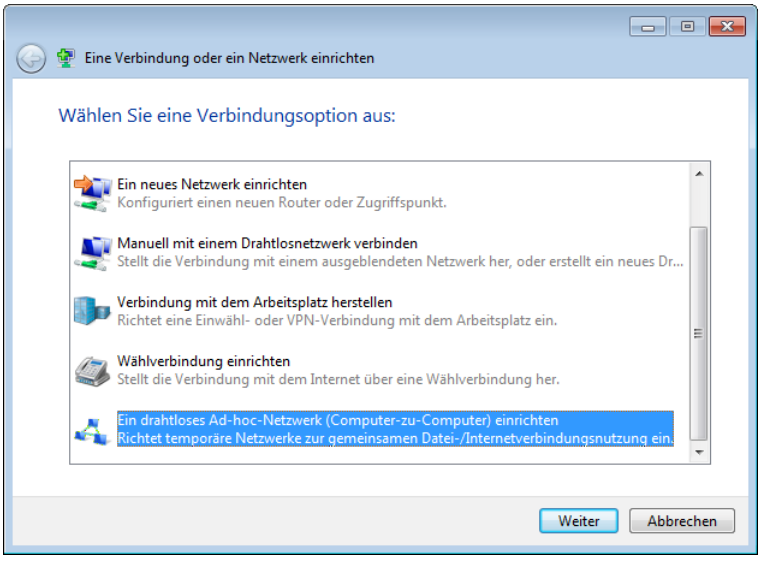

Eine Verbindung oder ein Netzwerk einrichten
Wählen Sie eine Verbindungsoption aus:
Ein neues Netzwerk einrichten
Konfiguriert einen neuen Router oder Zugriffspunkt.
Manuell mit einem Drahtlosnetzwerk verbinden
Stellt die Verbindung mit einem ausgeblendeten Netzwerk her, oder erstellt ein neues Dr...
Verbindung mit dem Arbeitsplatz herstellen
Richtet eine Einwähl- oder VPN-Verbindung mit dem Arbeitsplatz ein.
Wählverbindung einrichten
Stellt die Verbindung mit dem Internet über eine Wählverbindung her.
Ein drahtloses Ad-hoc-Netzwerk (Computer-zu-Computer) einrichten
Richtet temporäre Netzwerke zur gemeinsamen Datei-/Internetverbindungsnutzung ein.
Weiter
Abbrechen

Abbildung 6.45 Auswählen der Option *Ein drahtloses Ad-hoc-Netzwerk (Computer-zu-Computer) einrichten*

6. Öffnen Sie das Netzwerk- und Freigabecenter.
7. Klicken Sie auf *Neue Verbindung oder neues Netzwerk einrichten*.
8. Wählen Sie *Ein drahtloses Ad-hoc-Netzwerk (Computer-zu-Computer) einrichten* aus (Abbildung 6.45). Klicken Sie auf *Weiter*.
9. Klicken Sie auf *Weiter*, um die Seite *Ein drahtloses Ad-hoc-Netzwerk einrichten* zu überspringen.
10. Geben Sie den Netzwerknamen **MyAdHoc** ein, wählen Sie als Sicherheitstyp *WEP* aus und tragen Sie den Sicherheitsschlüssel **P@ss1** ein, wie in Abbildung 6.46 gezeigt. Klicken Sie auf *Weiter*.

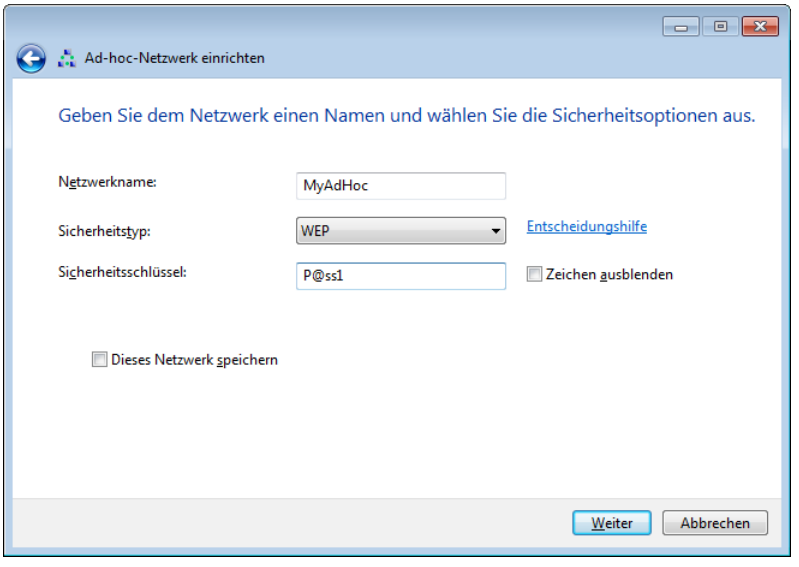


Abbildung 6.46 Konfigurieren des Ad-hoc-Netzwerks

11. Klicken Sie auf *Schließen*.
12. Klicken Sie im Netzwerk- und Freigabecenter auf *Verbindung mit einem Netzwerk herstellen*. Das Netzwerk *MyAdHoc* wird mit dem Status *Warten auf Benutzer* angezeigt.
13. Melden Sie sich mit einem Standardbenutzerkonto am Computer *Canberra* an.
14. Klicken Sie auf das Drahtlosnetzwerksymbol rechts unten auf Ihrem Bildschirm.
15. Klicken Sie mit der rechten Maustaste auf *MyAdHoc* und wählen Sie den Befehl *Verbinden*.
16. Geben Sie den Sicherheitsschlüssel ein (**P@ss1**).
17. Geben Sie im Suchfeld des Startmenüs **Aberdeen** ein. Stellen Sie sicher, dass Sie den freigegebenen Ordner *Test* angezeigt bekommen.
18. Klicken Sie auf das Drahtlosnetzwerksymbol rechts unten auf Ihrem Bildschirm.
19. Klicken Sie mit der rechten Maustaste auf *MyAdHoc* und wählen Sie den Befehl *Trennen*. Falls der Computer *Canberra* vorher mit einem anderen Netzwerk verbunden war, können Sie diese Verbindung nun wieder herstellen.

20. Trennen Sie den Computer *Aberdeen* vom Netzwerk *MyAdHoc*. Wie Sie sehen, wird das Netzwerk nun auf keinem der Computer mehr aufgelistet.

Zusammenfassung der Lektion

- Probleme mit Drahtloskonnektivität können auftreten, wenn sich ein Computer in der Reichweite zweier bevorzugter Netzwerke befindet oder zwei Netzwerke dieselbe SSID haben. Auch Störungen durch Haushaltsgeräte können Probleme verursachen. Sie können den vom WAP benutzten Kanal wechseln, um solche Störungen zu verringern.
- Wenn Sie ein ungeschütztes Drahtlosnetzwerk verwenden, kann das erhebliche Gefahren bergen. Stellen Sie beim Konfigurieren eines Drahtlosnetzwerks immer sicher, dass es geschützt ist.
- Sie können im Netzwerk- und Freigabecenter eine Verbindung zu einem Drahtlosnetzwerk herstellen, Drahtlosnetzwerke verwalten und einen Drahtlosadapter aktivieren oder deaktivieren. Sie können auch das Befehlszeilenprogramm `netsh wlan` verwenden, um Drahtlosnetzwerke zu verwalten.
- Windows 7 konfiguriert den Drucker, den Sie in einem bestimmten Netzwerk als Standarddrucker auswählen, immer als Standarddrucker, wenn Sie mit diesem Netzwerk verbunden sind. Wenn Sie daher zwischen Netzwerken wechseln, wird der Standarddrucker nahtlos umgestellt. Sie können standortabhängiges Drucken konfigurieren und Standarddrucker für jedes Netzwerk auswählen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 3, »Netzwerkkonfiguration«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Einer der Benutzer, für den Sie Support leisten, verwendet im Büro ein WLAN-fähiges Notebook, das er auch auf Geschäftsreisen mitnimmt. Er berichtet, dass häufig Verzögerungen und Verbindungsprobleme auftreten, wenn er das Notebook in der Lobby eines Hotels verwendet. Er hat keine Probleme, wenn er mit dem Notebook in seinem Hotelzimmer arbeitet oder ins Büro zurückkehrt. Wie sollten Sie das Problem lösen?
   A. Ändern Sie die SSID des Büronetzwerks.
   B. Raten Sie dem Benutzer, die Reihenfolge zu ändern, in der sein Notebook versucht, auf die bevorzugten Netzwerke zuzugreifen.
   C. Deaktivieren Sie die Netzwerkumschaltung bei einem oder beiden der bevorzugten Netzwerke, zu denen der Benutzer eine Verbindung herstellt, um im Hotel auf das Internet zuzugreifen.
   D. Aktualisieren Sie den Gerätetreiber für den WLAN-Adapter des Benutzers.

2. Sie wollen sicherstellen, dass nur bestimmte WLAN-Notebooks eine Verbindung mit Ihrem Netzwerk herstellen dürfen. Was müssen Sie aktivieren?
   A. MAC-Adressfilterung
   B. IPv4-Adressfilterung
   C. WEP
   D. WPA
3. Sie haben Probleme mit einer Verbindung und wollen die Windows-Netzwerkdiagnose ausführen. Wie können Sie auf dieses Tool zugreifen? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Wählen Sie im Menü *Zubehör* den Befehl *Systemprogramme*.
   B. Wählen Sie im Menü *Verwaltung* den Befehl *Aufgabenplanung*. Richten Sie den Zeitplan für das Netzwerkdiagnosetool so ein, dass es sofort gestartet wird.
   C. Klicken Sie im Netzwerk- und Freigabecenter auf das rote X, das auf einen Verbindungsfehler hinweist.
   D. Öffnen Sie das Dialogfeld *Eigenschaften von LAN-Verbindung* und klicken Sie auf *Konfigurieren*. Klicken Sie auf der Registerkarte *Allgemein* auf *Reparieren*.
   E. Klicken Sie in der Meldung, die der Browser anzeigt, wenn er nicht auf eine Webseite zugreifen kann, auf *Diagnose von Verbindungsproblemen*.
   F. Öffnen Sie das Dialogfeld *Netzwerkverbindungen*, indem Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern* klicken. Klicken Sie mit der rechten Maustaste auf eine Verbindung und wählen Sie den Befehl *Diagnose*.
4. Don Hall hat zu Hause ein Drahtlosnetzwerk eingerichtet. Er freut sich, wie einfach er den WAP in Betrieb nehmen kann: Er braucht lediglich eine einzige Schaltfläche in der Webschnittstelle anzuklicken. Seine Nachbarin erzählt ihm nun aber, dass sie von ihrem Heimcomputer aus auf sein Netzwerk zugreifen kann. Was sollte Don tun?
   A. Windows-Firewall aktivieren
   B. Die Sicherheitseinstellungen seines WAPs ändern
   C. Den von seinem WAP benutzten Kanal wechseln
   D. ICS einrichten
5. Sam Abolrous arbeitet bei der Firma A. Datum in ständig wechselnden Büroräumen. Wenn er an einem Schreibtisch im dritten Stock arbeitet, möchte er, dass alle seine Druckaufträge an den Drucker *LaserF3* gehen. Arbeitet er in einem Büro im ersten Stock, sollen die Druckaufträge an den Drucker *LaserF2* geleitet werden. Der dritte Stock des Gebäudes wird durch das Drahtlosnetzwerk *Adatum3* abgedeckt, der erste Stock vom Drahtlosnetzwerk *Adatum2*. Zwischen den Stockwerken befindet sich eine Abschirmung, sodass vom dritten Stock aus kein Zugriff auf das Netzwerk *Adatum2* möglich ist. Umgekehrt ist es auch nicht möglich, im ersten Stock auf das Netzwerk *Adatum3* zuzugreifen. Wie konfigurieren Sie das standortabhängige Drucken auf Sams Notebook, der unter Windows 7 Enterprise läuft?
   A. Wählen Sie *Immer den gleichen Drucker als Standarddrucker verwenden* aus. Wählen Sie in der Dropdownliste *Drucker* den Eintrag *LaserF2* aus.
   B. Wählen Sie *Immer den gleichen Drucker als Standarddrucker verwenden* aus. Wählen Sie in der Dropdownliste *Drucker* den Eintrag *LaserF3* aus.

C. Wählen Sie *Beim Ändern des Netzwerks den Standarddrucker ändern* aus. Stellen Sie *LaserF2* als Standarddrucker für das Netzwerk *Adatum3* ein und *LaserF3* als Standarddrucker für das Netzwerk *Adatum2*.

D. Wählen Sie *Beim Ändern des Netzwerks den Standarddrucker ändern* aus. Stellen Sie *LaserF2* als Standarddrucker für das Netzwerk *Adatum2* ein und *LaserF3* als Standarddrucker für das Netzwerk *Adatum3*.

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- IPv4 leitet Pakete innerhalb eines Subnetzes und über ein Intranet weiter. IPv6 führt dieselben Funktionen wie IPv4 aus, beseitigt aber viele Probleme des älteren Protokolls, darunter den knappen Adressraum.
- Im Netzwerk- und Freigabecenter und mit den Netsh-Befehlen können Sie Netzwerke und Netzwerkverbindungen konfigurieren und Verbindungen zu Netzwerken herstellen. Die Windows-Netzwerkdiagnose können Sie im Netzwerk- und Freigabecenter öffnen.
- Wichtige Befehlszeilentools für die Netzwerkdiagnose sind Ping, Tracert, Pathping und Netstat. Die Windows-Netzwerkdiagnose löst viele Netzwerkprobleme automatisch.
- Windows 7 bietet erweiterte Druckfunktionen, darunter das standortabhängige Drucken.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Standardgateway**
- **Globale Adresse**
- **IP-Adresse**
- **IP-Paket**
- **Bevorzugtes Drahtlosnetzwerk**
- **Öffentliche Adresse**
- **Subnetz**
- **Subnetzmaske**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie an, was Sie über Netzwerkeinstellungen gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Implementieren der IPv4-Konnektivität

Ein Freund betreibt von zu Hause aus ein Kleingewerbe. Bis vor Kurzem hat er einen einzigen Windows 7-Computer verwendet, der direkt an sein DSL-Modem angeschlossen war, sodass er auf das Internet zugreifen konnte. Die Geschäfte laufen gut und er verwendet inzwischen drei Computer. Er hat sie über einen Ethernetswitch miteinander verbunden, und das DSL-Modem ist über ein USB-Kabel angeschlossen.

Beantworten Sie die folgenden Fragen:

1. Ihr Freund ruft Sie an und erzählt, dass der Computer, an den das Modem angeschlossen ist, auf das Internet zugreifen kann, die anderen aber nicht. Was raten Sie ihm?
2. Bei einem weiteren Anruf erzählt Ihr Freund, dass er einen Drahtloscomputer und einen WAP gekauft hat. Er möchte wissen, wie er diesen Computer in seinem Netzwerk benutzen kann, ohne etwas an den drei Desktopcomputern zu verändern, die nur Kabelverbindungen haben. Was raten Sie ihm?

Übung mit Fallbeispiel 2: Implementieren der IPv6-Konnektivität

Sie sind Netzwerkadministrator bei Blue Sky Airlines. Ihr Unternehmensnetzwerk besteht aus zwei Subnetzen mit fortlaufenden privaten IPv4-Netzwerken, die als VLANs konfiguriert und mit einem Schicht-3-Switch verbunden sind. Blue Sky Airlines greift auf seinen Internetprovider und das Internet über einen mehrfach vernetzten Windows-Server zu, auf dem Microsoft ISA (Internet Security and Acceleration) läuft. Dieser Server stellt NAT- und Firewalldienste zur Verfügung und ist über eine periphere Zone mit einer Hardwarefirewall und darüber mit dem Internetprovider verbunden. Alle Arbeitsstationen der Benutzer laufen unter Windows 7 Enterprise. Das Unternehmen möchte IPv6-Konnektivität implementieren. Die gesamte Netzwerkhardware wie auch der Internetprovider unterstützen IPv6.

Beantworten Sie die folgenden Fragen:

1. Welche Unicastadresstypen können in den Subnetzen benutzt werden?
2. Sie wissen, dass auf Ihren Windows 7-Clients IPv6 in der Standardeinstellung aktiviert ist. Ihre standortlokalen Adressen werden über statusbehaftete Konfiguration (mit DHCPv6) zugewiesen, aber wenn Sie auf irgendeinem Clientcomputer **ipconfig /all** eingeben, bekommen Sie stets die Adresse 2001:: ce49:7601:e866:efff:f5ff:ebfe angezeigt. Welche Art Adresse ist das und welche Aufgabe hat sie?

Übung mit Fallbeispiel 3: Verwenden von Windows 7-Notebooks in Drahtlosnetzwerken

Sie sind Netzwerkadministrator bei Margie's Travel. Sie planen, demnächst alle Clientcomputer auf Notebooks umzustellen, die unter Windows 7 Enterprise laufen. Alle Clients stellen Drahtlosverbindungen her, und von den Angestellten wird erwartet, dass sie Drahtlosnetz-

werke zu Hause haben, damit sie sowohl im eigenen Arbeitszimmer als auch im Büro arbeiten können.

Beantworten Sie die folgenden Fragen:

1. Ein Manager macht sich ernste Sorgen, ob er ständig seinen Standarddrucker umschalten muss. Im Büro hat er einen anderen Drucker als den WLAN-Tintenstrahldrucker bei sich zu Hause. Was raten Sie ihm?
2. Derselbe Manager möchte seinen privaten Drucker durch ein neueres Modell ersetzen. Er bittet Sie, seinem Konto lokale Administratorprivilegien zuzuweisen, damit er den neuen Drucker installieren kann. Was sagen Sie ihm?
3. Die Hauptniederlassung von Margie's Travel hat zwei Drahtlosnetzwerke. Die Angestellten können sich normalerweise zwischen den beiden Bereichen bewegen, ohne dass die Verbindung verloren geht. Ein Angestellter beschwert sich nun, dass die Verbindung schlecht ist, während er am Schreibtisch sitzt. Befindet er sich dagegen am einen oder anderen Ende des Gebäudes, ist die Verbindung gut. Wie lösen Sie dieses Problem?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Konfigurieren von IPv4

- **Übung 1** Das vielseitige und leistungsfähige Netzwerk- und Freigabecenter bietet viele Möglichkeiten. Machen Sie sich gründlich mit allen seinen Funktionen und mit den Fenstern, Assistenten und Dialogfeldern vertraut.
- **Übung 2** Machen Sie sich mit allen Argumenten der Tools Ping, Tracert, Ipconfig, Pathping und Netstat vertraut. Verwenden Sie dazu die Befehlszeilenhilfe (zum Beispiel **ping /?**).
- **Übung 3** Simulieren Sie einige Probleme mit Ihren Schnittstellen (ziehen Sie beispielsweise Ethernetkabel ab und konfigurieren Sie Adapter falsch). Untersuchen Sie die Probleme mit der Windows-Netzwerkdiagnose.
- **Übung 4** Verwenden Sie in der Eingabeaufforderung die Hilfefunktion, um sich über die Befehle `netsh interface ipv4 set`, `netsh interface ipv4 add` und `netsh interface ipv4 show` zu informieren. Machen Sie sich auch mit den `netsh dhcp`-Befehlen vertraut.

Konfigurieren von IPv6

- **Übung 1** Sie sollten in der Lage sein, mit einem Blick auf eine IPv6-Adresse zu erkennen, ob es eine globale, verbindungslokale, standortlokale oder Multicastadresse ist. Teredo-, 6to4- und ISATAP-Adressen sind etwas schwieriger zu identifizieren, aber mit etwas Übung sollte Ihnen auch das gelingen. Sehen Sie sich dazu Listen mit Adressen an. Der Befehl `ipconfig /all` ist ein guter Ausgangspunkt.
- **Übung 2** Verwenden Sie in der Eingabeaufforderung die Hilfefunktion, um sich über die Befehle `netsh interface ipv6 set`, `netsh interface ipv6 add` und `netsh interface ipv6 show` zu informieren.

Konfigurieren von Netzwerken

- **Übung 1** Auch wenn Sie wahrscheinlich nicht jede Funktion nutzen, die in der Webkonfigurationsoberfläche eines WAP zur Verfügung steht, sollten Sie wissen, welche Einstellungen es für den Drahtloszugriff gibt. Machen Sie sich mit den Konfigurationsseiten (oder Registerkarten) vertraut. Arbeiten Sie dabei in der Weboberfläche und lesen Sie die Dokumentation des Herstellers.
- **Übung 2** Verwenden Sie in der Eingabeaufforderung die Hilfefunktion, um sich über die Befehle `netsh wlan add`, `netsh wlan connect`, `netsh wlan delete`, `netsh wlan disconnect`, `netsh wlan dump`, `netsh wlan export`, `netsh wlan refresh`, `netsh wlan reportissues`, `netsh wlan set`, `netsh wlan show`, `netsh wlan start` und `netsh wlan stop` zu informieren. Setzen Sie diese Befehle ein, um Drahtlosnetzwerke zu verwalten.
- **Übung 3** Windows 7 bietet Verbesserungen bei der Druckqualität und eine komfortablere Druckverwaltung. Machen Sie sich damit vertraut, welche Möglichkeiten im Fenster *Geräte und Drucker* zur Verfügung stehen.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

KAPITEL 7

Windows-Firewall und Remoteverwaltung

Firewalls sind wichtig. Von dem Moment an, an dem Ihr Computer eine Verbindung mit einem öffentlichen Netzwerk herstellt, suchen automatische Scanner an seinen Netzwerkschnittstellen nach Schwachstellen. Heutzutage verwenden viele Computerbenutzer gelegentlich öffentlich zugängliche Drahtlosnetzwerke, beispielsweise in einem Café oder Flughafen. Wenn Sie in einem Café eine Verbindung mit dem angebotenen Drahtlosnetzwerk herstellen, wissen Sie nicht, ob nicht ein paar Tische weiter jemand sitzt, der mit einem Portscanner nach Schwachstellen im Sicherheitssystem Ihres Computers sucht. Sie brauchen immer eine Firewall, nicht nur bei Verbindungen mit öffentlichen Netzwerken. Sie muss auch aktiv sein, wenn Sie eine Verbindung mit dem Netzwerk Ihres Unternehmens herstellen, weil Sie nicht wissen, ob zum Beispiel die Handelsvertreter mit ihren Laptops auf Reisen immer vorsichtig waren. Vielleicht ist einer der Laptops unterwegs infiziert worden. Wird dieser infizierte Computer wieder ans Netzwerk angeschlossen und einige der anderen Clients sind nicht durch Firewalls geschützt, wird es vermutlich nicht lange dauern, bis der infizierte Computer auch die anderen ungeschützten Computer im Netzwerk infiziert hat.

Da auch IT-Abteilungen immer mehr zu tun haben, bleibt den Mitarbeitern weniger Zeit, technische Probleme ihrer Kunden vor Ort zu beheben. Es wird immer wichtiger, so viele Probleme wie möglich per Fernwartung zu beheben, statt jeden Computer vor Ort zu untersuchen. Mit Windows 7 wird dies einfacher. Clients, auf denen Windows 7 verwendet wird, bieten nicht nur Remotedesktop und Windows-Remoteunterstützung, sondern es ist nun auch möglich, Windows PowerShell-Skripts und Befehlszeilenprogramme so auszuführen, dass sie auf den entsprechend konfigurierten Clients wirksam werden. Dadurch hat die Supportabteilung mehr Möglichkeiten bei der Behebung von Problemen.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren der Windows-Firewall
- Konfigurieren der Remoteverwaltung

Lektionen in diesem Kapitel:

- Lektion 1: Verwalten der Windows-Firewall 381
- Lektion 2: Windows 7-Remoteverwaltung 400

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels sind einige Vorbereitungen erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Client-PC namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.
- Sie haben Windows 7 auf einem eigenständigen Client-PC namens *Aberdeen* installiert, wie in Kapitel 6, »Netzwerkeinstellungen«, beschrieben.

Praxistipp

Orin Thomas

Wahrscheinlich war es gar nicht so schlecht für mich, dass die Remoteverwaltung noch in den Kinderschuhen steckte, als ich im Support arbeitete. Als ich damals an einer Universität in Australien Supportmitarbeiter war, musste ich mich viel auf einem sehr großen Campus bewegen, um Leuten in weit auseinander liegenden Gebäuden bei ihren Computerproblemen zu helfen. Obwohl ich auf meinem Weg zu einem streikenden Computer am Donut-Shop vorbeikam, ging es mir doch wesentlich besser, da ich mich viel an der frischen Luft bewegte. Müsste ich diese Arbeit heute machen, mit der Unmenge an Remoteunterstützungstechnologie, die in Windows 7 verfügbar ist, würde ich meinen Schreibtisch wohl kaum noch verlassen. Statt von meinem Büro beispielsweise zu den Soziologen zu gehen, um jemanden bei dem Problem »dieses E-Mail-Dings tut dies und das nicht« zu helfen, könnte ich per Remoteunterstützung genau das sehen, was auch der betreffende Benutzer sieht, und ihm die Bedienung des Programms genauer erklären. Ich könnte viele Routinearbeiten mit Remotedesktop oder Windows PowerShell erledigen, statt von Büro zu Büro zu gehen, um Updates zu installieren und Konfigurationseinstellungen manuell vorzunehmen. Hätte es die heutige Remoteverwaltungstechnologie damals schon gegeben, hätte ich vermutlich nur noch am Schreibtisch gesessen und nicht viel Bewegung gehabt.

Lektion 1: Verwalten der Windows-Firewall

Die Firewall aus dem Lieferumfang von Windows 7 hat die Aufgabe, Ihren Computer zu schützen. Sie schützt Ihren Computer nicht nur, wenn er mit dem geschützten Netzwerk im Büro verbunden ist, sondern auch dann, wenn er mit dem weniger sicheren öffentlichen Drahtlosnetzwerk eines Cafés oder eines Flughafens verbunden ist. In dieser Lektion erfahren Sie etwas über den Unterschied zwischen der Windows-Firewall und der Windows-Firewall mit erweiterter Sicherheit. Außerdem werden die Verbindungssicherheitsregeln beschrieben, mit denen Sie die Netzwerkkommunikation Ihres Computers beschränken können, damit zum Beispiel nur noch Verbindungen zu Computern zugelassen werden, die ihre Identität bewiesen haben.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren von Regeln für mehrere Profile
- Zulassen oder Ablehnen von Anwendungen
- Erstellen von netzwerkprofilspezifischen Regeln
- Konfigurieren von Benachrichtigungen
- Konfigurieren von Authentifizierungsausnahmen

Veranschlagte Zeit für diese Lektion: 40 Minuten

Windows-Firewall

Firewalls beschränken den Netzwerkdatenverkehr auf der Basis einer Sammlung von konfigurierbaren Regeln. Diese Regeln werden auch *Ausnahmen* (exceptions) genannt. Wenn Netzwerkdatenverkehr eine Netzwerkschnittstelle erreicht, die durch eine Firewall geschützt ist, untersucht die Firewall die Daten und entscheidet mit den konfigurierten Regeln, ob die Daten verworfen oder zugelassen werden. Windows 7 setzt zwei Firewalls ein, die zusammenarbeiten: die Windows-Firewall und die Windows-Firewall mit erweiterter Sicherheit (Windows Firewall with Advanced Security, WFAS). Der wichtigste Unterschied zwischen diesen Firewalls besteht in der Komplexität der Regeln. Die Windows-Firewall verwendet einfache Regeln, die sich direkt auf ein Programm oder einen Dienst beziehen. WFAS lässt komplexere Regeln zu, die den Datenverkehr auf der Basis von Port, Protokoll, Adresse und Authentifizierung filtern. WFAS wird in dieser Lektion später ausführlicher besprochen.

Zum Verständnis der Funktionsweise von Firewallregeln ist Folgendes wichtig: Wenn es keine Regel gibt, die eine bestimmte Form des Datenverkehrs zulässt, verwirft die Firewall die betreffenden Daten. Im Allgemeinen müssen Sie Datenverkehr explizit zulassen, damit er die Firewall durchlaufen kann. Gelegentlich wird es aber erforderlich sein, eine Ablehnungsregel zu konfigurieren. Über Ablehnungsregeln erfahren Sie mehr im Verlauf dieser Lektion. Die Windows-Firewall und WFAS werden mit einer kleinen Anzahl von Standardregeln für die Arbeit im Netzwerk ausgeliefert. Mit diesen Regeln können Sie zwar im Internet arbeiten, ohne eine Firewallregel zu konfigurieren, aber wenn Sie eine Anwendung wie *ftp.exe* verwenden (*ftp* steht für File Transfer Protocol), die ohne passende Standardregel Arbeiten im Netzwerk ausführen will, erscheint ein Dialogfeld mit einer Warnung. Darin unterscheidet sich Windows 7 von älteren Windows-Versionen wie Windows XP, bei denen die Firewall nur eingehenden Datenverkehr blockiert hat, ausgehenden aber nicht. Die Firewall von Windows 7 blockiert standardmäßig den größten Teil des ausgehenden Datenver-

kehrs. Wird ein Programm das erste Mal blockiert, werden Sie von der Firewall informiert (Abbildung 7.1) und können eine Ausnahme konfigurieren, die zukünftig Datenübertragungen von dieser Anwendung zulässt.

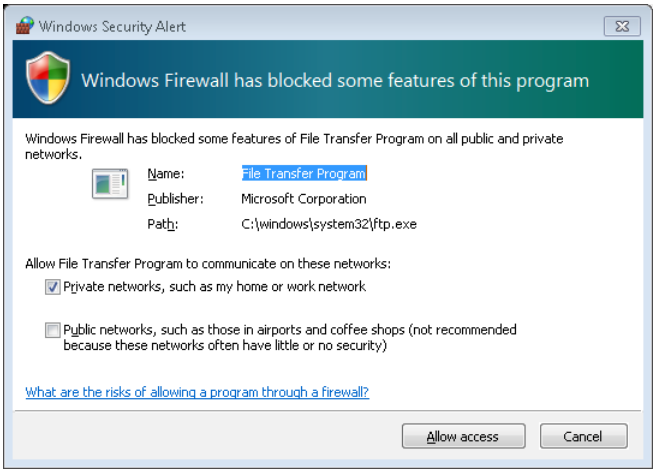

Windows Security Alert
Windows Firewall has blocked some features of this program
Windows Firewall has blocked some features of File Transfer Program on all public and private networks.
Name: File Transfer Program
Publisher: Microsoft Corporation
Path: C:\windows\system32\ftp.exe
Allow File Transfer Program to communicate on these networks:
Private networks, such as my home or work network
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)
What are the risks of allowing a program through a firewall?
Allow access
Cancel

Abbildung 7.1 Der meiste ausgehende Datenverkehr wird blockiert und in Form einer Warnung gemeldet

Die Windows 7-Firewall verwendet eine Funktion, die »full stealth« genannt und in der deutschen Dokumentation auch als *geschützter Modus* bezeichnet wird. Die Stealth-Funktion hindert externe Hosts daran, einen Fingerabdruck des Betriebssystems zu erfassen (engl: OS fingerprinting). Damit ist eine Methode gemeint, mit der ein Angreifer herauszufinden versucht, welches Betriebssystem ein Computer verwendet, indem er spezielle Daten an die externe Netzwerkschnittstelle des Computers sendet. Sobald ein Angreifer weiß, welches Betriebssystem auf einem bestimmten Computer verwendet wird, kann er betriebssystemspezifische Angriffe auf den Computer durchführen. Die Stealth-Funktion von Windows 7 lässt sich nicht deaktivieren.

Die Startzeitfilterung (boot time filtering), eine weitere Funktion von Windows 7, sorgt dafür, dass die Windows-Firewall vom ersten Moment an arbeitet, an dem die Netzwerkschnittstellen aktiv werden. In älteren Betriebssystemen wie Windows XP waren die integrierte Firewall und auch Firewalls von anderen Herstellern erst betriebsbereit, nachdem das Betriebssystem hochgefahren war. Dadurch ergab sich eine kurze, aber wichtige Zeitspanne, in der eine Netzwerkschnittstelle bereits aktiv, aber noch nicht durch eine Firewall geschützt war. Die Startzeitfilterung schließt dieses Fenster.

Um die Arbeitsweise der Windows-Firewall zu verstehen, müssen Sie einige Grundkonzepte der Computervernetzung kennen. Falls Sie sich schon gut mit Netzwerken auskennen, können Sie den folgenden Text überspringen und mit dem nächsten Abschnitt fortfahren, weil Sie die folgenden Konzepte vermutlich bereits kennen:

- **Protokoll** Für die Windows-Firewall sind nur drei Protokolle von Interesse: TCP (Transmission Control Protocol), UDP (User Datagram Protocol) und ICMP (Internet Control Message Protocol). TCP ist zuverlässiger und wird für den größten Teil des Internetdatenverkehrs verwendet. UDP wird für Broadcast- und Multicastdaten sowie für Onlinespiele verwendet. ICMP dient hauptsächlich diagnostischen Zwecken.

- **Port** Ein Port ist eine Identifikationsnummer, die im Header eines TCP- oder UDP-Datagramms angegeben wird. Ports dienen zur Verknüpfung des Netzwerkdatenverkehrs mit bestimmten Diensten oder Programmen, die auf einem Computer ausgeführt werden. Port 80 ist zum Beispiel für den Datenverkehr mit dem World Wide Web reserviert und Port 25 für Übertragungen von E-Mails über das Internet.
- **IPSec (Internet Protocol Security)** IPSec ist eine Methode zur Sicherung des Netzwerkdatenverkehrs durch Verschlüsselung und Signatur. Die Verschlüsselung bewirkt, dass ein Angreifer abgefangenen Datenverkehr nicht lesen kann. Die Signatur bestätigt dem Empfänger die Identität des Absenders.
- **Netzwerkadresse** Jeder Host eines Netzwerks hat seine eigene Netzwerkadresse. Sie können Firewalls so konfigurieren, dass der Datenverkehr je nach dem Zielnetzwerk des ausgehenden Datenverkehrs oder dem Ursprungsnetzwerk des eingehenden Datenverkehrs unterschiedlich behandelt wird.
- **Eingehender Datenverkehr** Eingehender Datenverkehr ist der Netzwerkdatenverkehr, der von einem externen Host stammt und an Ihren Windows 7-Clientcomputer gerichtet ist.
- **Ausgehender Datenverkehr** Ausgehender Datenverkehr ist der Datenverkehr, den Ihr Windows 7-Client über das Netzwerk an externe Hosts sendet.
- **Netzwerkschnittstelle** Eine Netzwerkschnittstelle eignet sich dazu, eine direkte Verbindung mit dem LAN (Local Area Network), eine Drahtlosverbindung, eine Modemverbindung oder eine VPN-Verbindung (Virtual Private Network) herzustellen.

Erkennen der Netzwerkstandortkategorie (Network Location Awareness, NLA)

Windows 7 erkennt an den Eigenschaften einer Netzwerkverbindung, zu welcher Standortkategorie das Netzwerk gehört, und verwendet das dazu passende Netzwerkprofil. Wie Abbildung 7.2 zeigt, verwendet Windows 7 drei Netzwerkprofile: *Domänennetzwerke*, *Heim- oder Arbeitsplatznetzwerke (privat)* und *Öffentliche Netzwerke*. Wenn Sie eine Verbindung mit einem neuen Netzwerk herstellen, fragt Windows 7 Sie mit einem Dialogfeld, ob es sich bei dem Netzwerk um ein Heimnetzwerk, ein Arbeitsplatznetzwerk oder ein öffentliches Netzwerk handelt. Windows 7 merkt sich den Netzwerktyp, den Sie angeben, und verknüpft ihn mit den Eigenschaften des Netzwerks, damit der Typ bei der nächsten Verbindung mit dem Netzwerk wieder eingestellt werden kann. Den Netzwerktyp können Sie im Netzwerk- und Freigabecenter ändern. Wie das geschieht, haben Sie bereits in Kapitel 6 erfahren. NLA weist ein Domänennetzwerkprofil zu, wenn Sie sich bei einer Domäne der Active Directory-Domänendienste anmelden.

Netzwerkprofile sind wichtig, weil sie die Anwendung von verschiedenen Sammlungen von Firewallregeln ermöglichen. Abbildung 7.3 zeigt eine Konfiguration, bei der die Ausnahmeregel für Windows Virtual PC in den Profilen *Domäne* und *Heim/Arbeit (Privat)* aktiv ist, aber nicht im Profil *Öffentlich*. Ein wichtiger Unterschied zwischen Windows Vista und Windows 7 besteht darin, dass Windows 7-Profile auf Netzwerkschnittstellenbasis gelten. Das bedeutet, dass durchaus verschiedene Regelsätze gelten können, wenn über eine Netzwerkkarte eine Verbindung mit dem Internet besteht und über eine zweite Netzwerkkarte eine Verbindung mit dem Büro-LAN. Wenn ein Computer Verbindungen mit verschiedenen Netzwerktypen hergestellt hat, wählt die Firewall in Windows Vista das restriktivste Netzwerkprofil und wendet den restriktivsten Regelsatz auf alle Schnittstellen an.

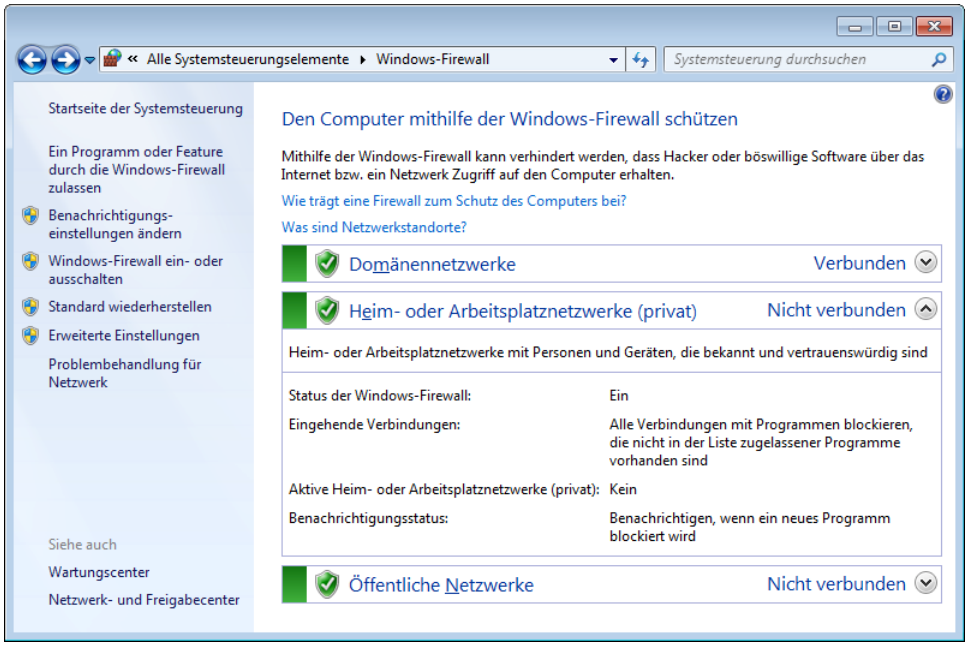

« Alle Systemsteuerungselemente ▸ Windows-Firewall
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Ein Programm oder Feature durch die Windows-Firewall zulassen
Benachrichtigungseinstellungen ändern
Windows-Firewall ein- oder ausschalten
Standard wiederherstellen
Erweiterte Einstellungen
Problembehandlung für Netzwerk
Siehe auch
Wartungscenter
Netzwerk- und Freigabecenter
Den Computer mithilfe der Windows-Firewall schützen
Mithilfe der Windows-Firewall kann verhindert werden, dass Hacker oder böswillige Software über das Internet bzw. ein Netzwerk Zugriff auf den Computer erhalten.
Wie trägt eine Firewall zum Schutz des Computers bei?
Was sind Netzwerkstandorte?
Domänennetzwerke
Verbunden
Heim- oder Arbeitsplatznetzwerke (privat)
Nicht verbunden
Heim- oder Arbeitsplatznetzwerke mit Personen und Geräten, die bekannt und vertrauenswürdig sind
Status der Windows-Firewall: Ein
Eingehende Verbindungen: Alle Verbindungen mit Programmen blockieren, die nicht in der Liste zugelassener Programme vorhanden sind
Aktive Heim- oder Arbeitsplatznetzwerke (privat): Kein
Benachrichtigungsstatus: Benachrichtigen, wenn ein neues Programm blockiert wird
Öffentliche Netzwerke
Nicht verbunden

Abbildung 7.2 Die Windows-Firewall in der Systemsteuerung

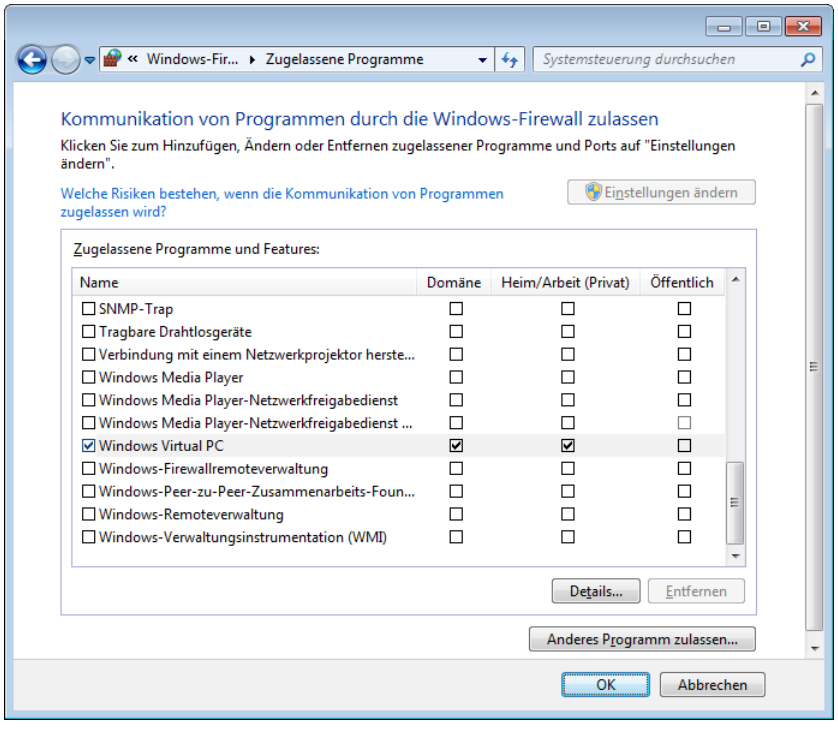


Abbildung 7.3 Zulassen von Programmen und Funktionen in verschiedenen Profilen

Sie können die Windows-Firewall für jedes Netzwerkprofil separat aktivieren (Abbildung 7.4). Außerdem können Sie festlegen, ob der angemeldete Benutzer benachrichtigt werden soll, wenn die Windows-Firewall ein neues Programm blockiert, und ob alle eingehenden Verbindungen blockiert werden sollen, einschließlich der durch Firewallregeln zugelassenen Verbindungen. Allerdings können Benutzer nur dann über den Datenverkehr Regeln erstellen, über den sie informiert werden, wenn sie über die Berechtigungen eines lokalen Administrators verfügen.

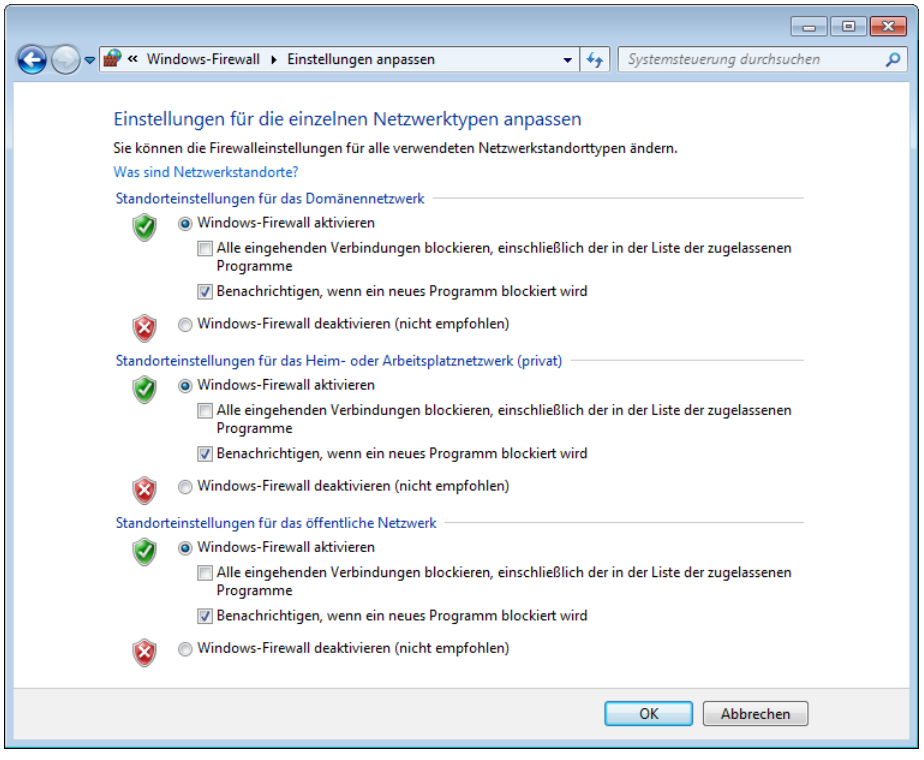

« Windows-Firewall ▸ Einstellungen anpassen
Systemsteuerung durchsuchen
Einstellungen für die einzelnen Netzwerktypen anpassen
Sie können die Firewalleinstellungen für alle verwendeten Netzwerkstandorttypen ändern.
Was sind Netzwerkstandorte?
Standorteinstellungen für das Domänennetzwerk
Windows-Firewall aktivieren
Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Programme
Benachrichtigen, wenn ein neues Programm blockiert wird
Windows-Firewall deaktivieren (nicht empfohlen)
Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)
Windows-Firewall aktivieren
Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Programme
Benachrichtigen, wenn ein neues Programm blockiert wird
Windows-Firewall deaktivieren (nicht empfohlen)
Standorteinstellungen für das öffentliche Netzwerk
Windows-Firewall aktivieren
Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Programme
Benachrichtigen, wenn ein neues Programm blockiert wird
Windows-Firewall deaktivieren (nicht empfohlen)
OK
Abbrechen

Abbildung 7.4 Selektives Aktivieren der Windows-Firewall

Der wichtigste Grund, die Windows-Firewall in allen Profilen zu deaktivieren, ist die Verwendung einer Firewall von einem anderen Hersteller. In dieser Situation deaktivieren Sie die Windows-Firewall, damit die andere Firewall den Computer schützen kann. Deaktivieren Sie die Windows-Firewall aber nicht einfach deswegen, weil es zwischen Ihrem Windows 7-Client und dem Internet noch eine andere Firewall gibt, beispielsweise in Form einer Hardwarefirewall oder eines SOHO-Routers (Small Office/Home Office). Es ist möglich, dass Malware bereits einen anderen Computer in Ihrem lokalen Netzwerk infiziert hat. Es empfiehlt sich, alle Netzwerke aus Sicherheitsgründen als potenziell feindlich einzustufen.

Zulassen von Programmen in der Windows-Firewall

Die Windows-Firewall ermöglicht die Konfiguration von Ausnahmen auf der Basis von Anwendungen. Unter Windows Vista war es dagegen auch möglich, Ausnahmen auf der Basis der Portadresse festzulegen. Das ist auch unter Windows 7 noch möglich, allerdings nur in der Windows-Firewall mit erweiterter Sicherheit, die später in dieser Lektion bespro-

chen wird. Sie können auch bestimmte Windows 7-Funktionen wie Windows Virtual PC zulassen. Funktionsregeln werden verfügbar, wenn Sie die Funktion in der Systemsteuerung unter *Programme und Funktionen* aktivieren. Um eine Regel für eine Funktion oder ein Programm hinzuzufügen, klicken Sie im Abschnitt *Windows-Firewall* der Systemsteuerung auf *Ein Programm oder Feature durch die Windows-Firewall zulassen*. Das bereits in Abbildung 7.3 gezeigte Dialogfeld zeigt eine Liste der installierten Funktionen und alle Programme an, für die Regeln erstellt wurden, und es zeigt, für welche Profile die Regeln gelten.

Wenn Sie auf dieser Seite Einstellungen ändern möchten, müssen Sie auf die Schaltfläche *Einstellungen ändern* klicken. Nur Benutzer, die Mitglieder der lokalen Gruppe *Administratoren* sind oder denen die entsprechenden Rechte zugewiesen wurden, können Windows-Firewall-Einstellungen ändern. Wird ein Programm, für das Sie eine Regel erstellen möchten, nicht in der Liste aufgeführt, klicken Sie auf *Anderes Programm zulassen*. Dadurch öffnet sich das Dialogfeld *Programm hinzufügen* (Abbildung 7.5). Falls das Programm, für das Sie eine Regel erstellen möchten, nicht aufgeführt wird, klicken Sie auf *Durchsuchen* und fügen es hinzu. Klicken Sie auf die Schaltfläche *Netzwerkstandorttypen*, wenn Sie festlegen möchten, in welchen Netzwerkprofilen die Regel aktiv sein soll.

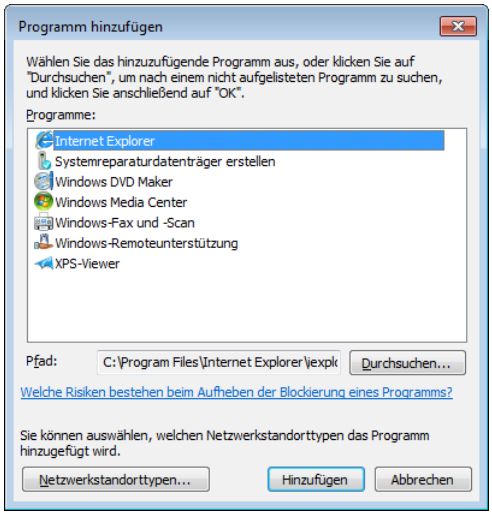


Abbildung 7.5 Hinzufügen einer Programmausnahme



Hinweis Rücksetzen der Firewall auf die Standardkonfiguration

Um die Windows-Firewall und WFAS auf ihre Standardkonfiguration zurückzusetzen, können Sie in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `netsh advfirewall reset` verwenden. Außerdem können Sie die Windows-Firewall und WFAS auf der Seite *Windows-Firewall* der Systemsteuerung mit einem Klick auf *Standard wiederherstellen* zurücksetzen.

Schnelltest

- Auf welcher Basis können Sie Regeln für die Windows-Firewall erstellen (im Gegensatz zu WFAS)?

Antwort zum Schnelltest

- Für die Windows-Firewall können Sie nur auf der Basis von Programmen und Windows 7-Funktionen Regeln erstellen, aber nicht auf der Basis einer Portadresse oder eines Dienstes.

Die Windows-Firewall mit erweiterter Sicherheit

Die Windows-Firewall mit erweiterter Sicherheit (Windows Firewall with Advanced Security, WFAS) ermöglicht Ihnen die Erstellung von komplexeren Regeln. Für die meisten Benutzer reichen die in der Windows-Firewall verfügbaren Optionen aus, um ihre Computer zu schützen. Fortgeschrittene können WFAS für folgende Aufgaben verwenden:

- Konfigurieren eingehender und ausgehender Regeln. Die Windows-Firewall unterscheidet bei der Erstellung von Regeln nicht zwischen eingehendem und ausgehendem Datenverkehr.
- Konfigurieren von Regeln auf der Basis von Protokolltyp und Portadresse.
- Konfigurieren von Regeln auf der Basis von bestimmten Diensten, nicht nur von bestimmten Anwendungen.
- Beschränken des Wirkungsbereichs von Regeln auf der Basis der Adressen des Absenders oder des Empfängers.
- Konfigurieren von Regeln, die nur authentifizierten Datenverkehr zulassen.
- Konfigurieren von Verbindungssicherheitsregeln.

Um die WFAS-Konsole zu öffnen, können Sie im Textfeld *Programme/Dateien durchsuchen* des *Start*-Menüs **Windows-Firewall mit erweiterter Sicherheit** eingeben oder auf der Seite *Windows-Firewall* der Systemsteuerung auf *Erweiterte Einstellungen* klicken. Die WFAS-Konsole zeigt an, welche Netzwerkprofile aktiv sind. Wie bei der Windows-Firewall können sich die Regelsätze unterscheiden, je nachdem, welches Netzwerkprofil für eine bestimmte Netzwerkkarte gilt. Abbildung 7.6 zeigt zum Beispiel eine Konfiguration mit aktivem Domänenprofil und aktivem öffentlichen Profil. Die beiden Profile sind in diesem Fall aktiv, weil der Computer, von dem das Bild stammt, über seine Drahtlosnetzwerkkarte mit einem Domänennetzwerk und über ein USB-Modem (Universal Serial Bus) mit dem Internet verbunden ist. Sie könnten nun eine Regel aktivieren, die im Domänenprofil Datenverkehr über Port 80 zulässt, aber nicht im öffentlichen Profil. Das würde bedeuten, dass Hosts, die über die Drahtlosnetzwerkkarte eine Verbindung mit diesem Computer herstellen, auf den Webserver zugreifen könnten, der auf dem Computer betrieben wird, während der Zugriff über die Internetverbindung auf denselben Webserver gesperrt ist.

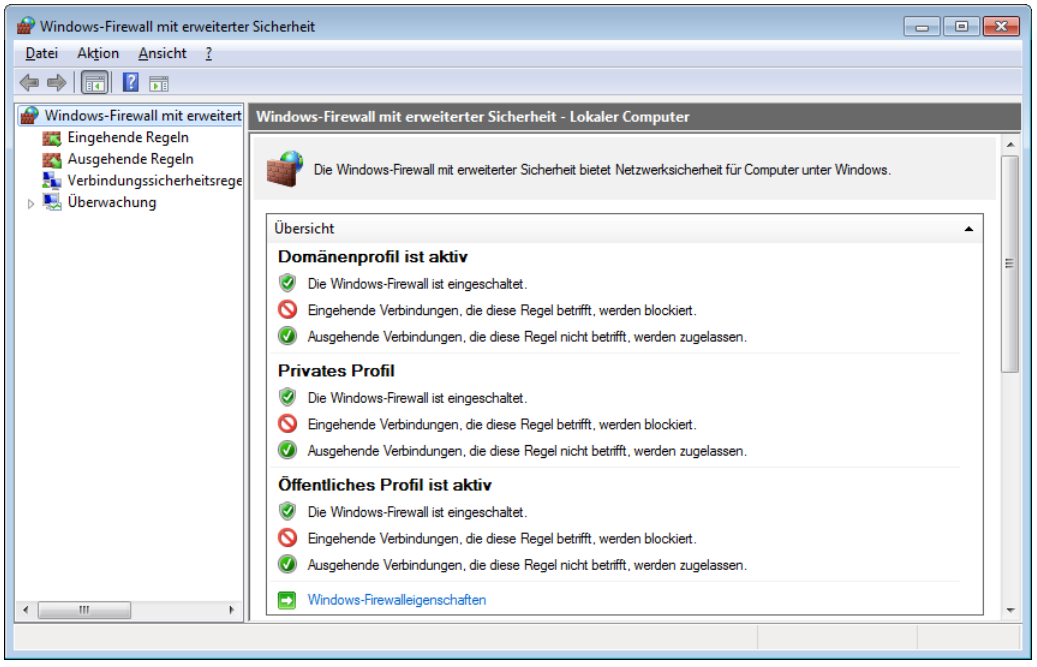

Windows-Firewall mit erweiterter Sicherheit
Datei Aktion Ansicht ?
Windows-Firewall mit erweitert
Eingehende Regeln
Ausgehende Regeln
Verbindungssicherheitsrege
Überwachung
Windows-Firewall mit erweiterter Sicherheit - Lokaler Computer
Die Windows-Firewall mit erweiterter Sicherheit bietet Netzwerksicherheit für Computer unter Windows.
Übersicht
Domänenprofil ist aktiv
Die Windows-Firewall ist eingeschaltet.
Eingehende Verbindungen, die diese Regel betrifft, werden blockiert.
Ausgehende Verbindungen, die diese Regel nicht betrifft, werden zugelassen.
Privates Profil
Die Windows-Firewall ist eingeschaltet.
Eingehende Verbindungen, die diese Regel betrifft, werden blockiert.
Ausgehende Verbindungen, die diese Regel nicht betrifft, werden zugelassen.
Öffentliches Profil ist aktiv
Die Windows-Firewall ist eingeschaltet.
Eingehende Verbindungen, die diese Regel betrifft, werden blockiert.
Ausgehende Verbindungen, die diese Regel nicht betrifft, werden zugelassen.
Windows-Firewalleigenschaften

Abbildung 7.6 Die WFAS-Konsole zeigt mehrere aktive Netzwerkprofile

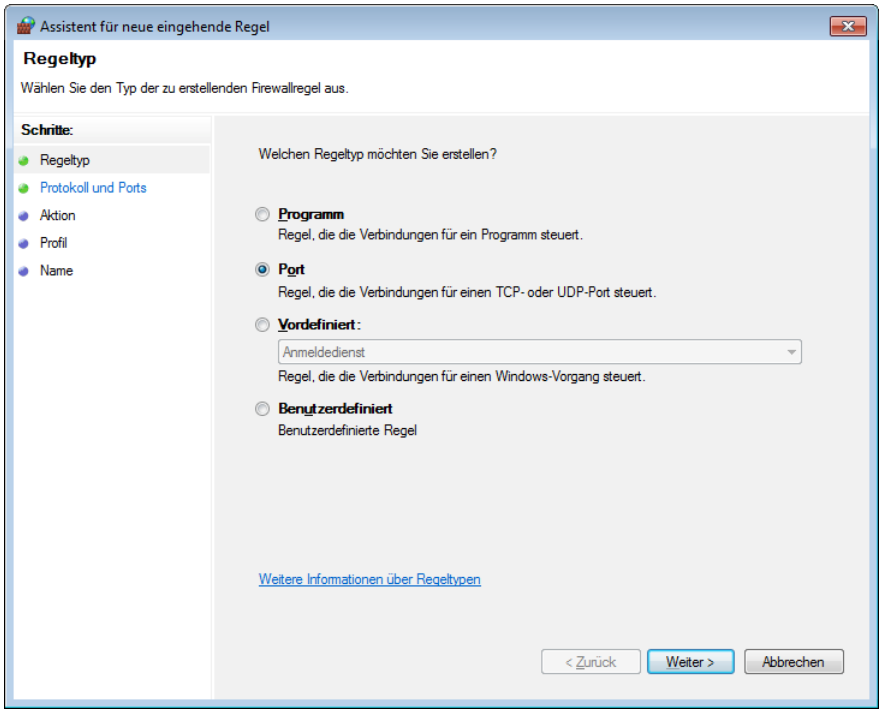


Abbildung 7.7 Der Assistent für neue eingehende Regel

Erstellen von WFAS-Regeln

Die Konfiguration eingehender und ausgehender Regeln erfolgt im Wesentlichen in derselben Weise: Sie wählen in der WFAS-Konsole den Knoten aus, der für den zu erstellenden Regeltyp steht, und klicken dann im Aktionsbereich auf *Neue Regel*. Dadurch öffnet sich der Assistent für neue eingehende (oder ausgehende) Regeln. Auf der ersten Seite legen Sie den zu erstellenden Regeltyp fest (Abbildung 7.7). Sie haben die Wahl zwischen einer Programm-, einer Port-, einer vordefinierten oder einer benutzerdefinierten Regel. Die Programmregeln und die vordefinierten Regeln ähneln den Regeln, die Sie in der Windows-Firewall erstellen können. In einer benutzerdefinierten Regel können Sie Kriterien verwenden, die unter den anderen Optionen nicht verfügbar sind. Eine benutzerdefinierte Regel würden Sie zum Beispiel erstellen, wenn die Regel nicht für ein bestimmtes Programm oder einen bestimmen Port, sondern für einen bestimmten Dienst gelten soll. Außerdem können Sie eine benutzerdefinierte Regel verwenden, wenn die Regel für ein bestimmtes Programm und bestimmte Ports gelten soll. Wollen Sie zum Beispiel die Kommunikation mit einem bestimmten Programm über einen bestimmten Port zulassen, aber nicht über andere Ports, erstellen Sie eine benutzerdefinierte Regel.

Wenn Sie eine Programmregel erstellen möchten, müssen Sie ein bestimmtes Programm angeben, für das die Regel gelten soll. Wenn Sie eine Portregel wählen, müssen Sie festlegen, ob die Regel für das TCP- oder das UDP-Protokoll gelten soll. Außerdem müssen Sie Portnummern angeben. Im nächsten Schritt legen Sie fest, was mit dem Datenverkehr geschehen soll, der zu der Regel passt. Folgende Optionen stehen zur Wahl:

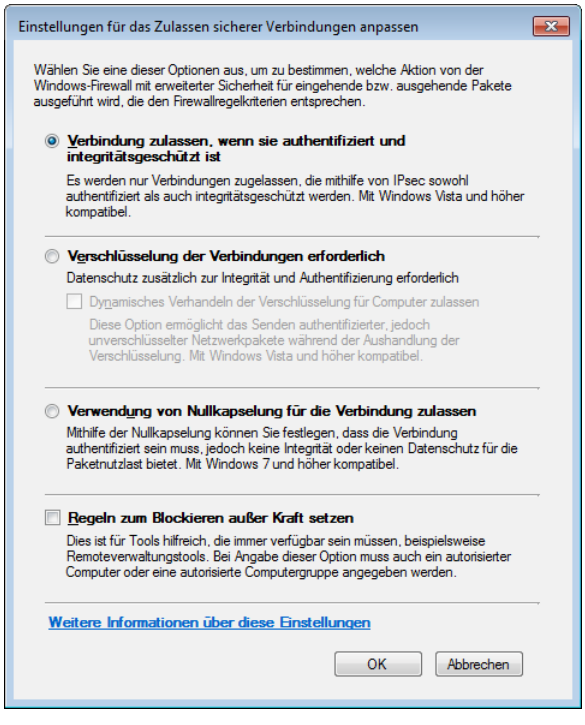

Einstellungen für das Zulassen sicherer Verbindungen anpassen
Wählen Sie eine dieser Optionen aus, um zu bestimmen, welche Aktion von der Windows-Firewall mit erweiterter Sicherheit für eingehende bzw. ausgehende Pakete ausgeführt wird, die den Firewallregelkriterien entsprechen.
Verbindung zulassen, wenn sie authentifiziert und integritätsgeschützt ist
Es werden nur Verbindungen zugelassen, die mithilfe von IPsec sowohl authentifiziert als auch integritätsgeschützt werden. Mit Windows Vista und höher kompatibel.
Verschlüsselung der Verbindungen erforderlich
Datenschutz zusätzlich zur Integrität und Authentifizierung erforderlich
Dynamisches Verhandeln der Verschlüsselung für Computer zulassen
Diese Option ermöglicht das Senden authentifizierter, jedoch unverschlüsselter Netzwerkpakete während der Aushandlung der Verschlüsselung. Mit Windows Vista und höher kompatibel.
Verwendung von Nullkapselung für die Verbindung zulassen
Mithilfe der Nullkapselung können Sie festlegen, dass die Verbindung authentifiziert sein muss, jedoch keine Integrität oder keinen Datenschutz für die Paketnutzlast bietet. Mit Windows 7 und höher kompatibel.
Regeln zum Blockieren außer Kraft setzen
Dies ist für Tools hilfreich, die immer verfügbar sein müssen, beispielsweise Remoteverwaltungstools. Bei Angabe dieser Option muss auch ein autorisierter Computer oder eine autorisierte Computergruppe angegeben werden.
Weitere Informationen über diese Einstellungen
OK
Abbrechen

Abbildung 7.8 Einstellen der Sicherheitsoptionen

- **Verbindung zulassen** WFAS lässt die Verbindung zu, wenn der Datenverkehr zu der Regel passt.
- **Verbindung blocken** WFAS blockiert die Verbindung, wenn der Datenverkehr zu der Regel passt.
- **Verbindung zulassen, wenn sie sicher ist** WFAS lässt die Verbindung zu, wenn der Datenverkehr zu der Regel passt und mit einer der Methoden authentifiziert wird, die in den Verbindungssicherheitsregeln festgelegt sind. Abbildung 7.8 zeigt die Sicherheitsoptionen.

Die Standardeinstellung setzt voraus, dass die Verbindung authentifiziert und integritätsgeschützt, aber unverschlüsselt ist. Verwenden Sie die Option *Verschlüsselung der Verbindungen erforderlich*, wenn die Firewallregeln nicht nur die Authentifizierung und den Integritätsschutz, sondern auch eine Verschlüsselung der Daten verlangen sollen. Mit der Option *Regeln zum Blockieren außer Kraft setzen* können Sie ein Computerkonto oder eine Computergruppe angeben, für die eine Blockierungsregel nicht gelten soll.

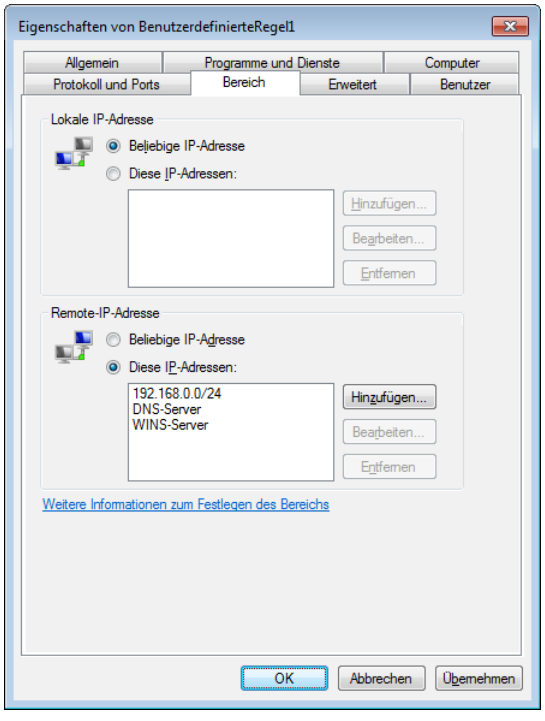


Abbildung 7.9 Konfigurieren des Regelbereichs

Regelbereich

Mit einem Regelbereich können Sie festlegen, ob eine Regel für bestimmte Quell- und Zieladressen gilt. Wenn Sie zum Beispiel eine Regel erstellen wollen, die eine bestimmte Art von Datenverkehr nur für bestimmte Netzwerkadressen zulässt, müssen Sie den Bereich der Regel ändern. Bei der Erstellung einer Regel können Sie den Bereich aber nur für benutzerdefinierte Regeln festlegen, nicht für Programm- oder Portregeln. Für diese Regeltypen können Sie den Bereich nach der Erstellung im Eigenschaftendialogfeld der Regel angeben

(Abbildung 7.9). Sie können IP-Adressen (Internet Protocol), IP-Adressbereiche oder einen der vordefinierten Computersätze *Standardgateway*, *WINS-Server*, *DHCP-Server*, *DNS-Server* oder *Lokales Subnetz* angeben. Zur Angabe der Adressen und Adressbereiche können Sie IPv4- und IPv6-Adressen verwenden.

So ändern Sie nachträglich den Bereich einer Regel:

1. Klicken Sie die Regel in der WFAS-Konsole mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Dadurch öffnet sich das Eigenschaftendialogfeld der Regel. Klicken Sie auf die Registerkarte *Bereich*.
2. Wenn Sie die lokalen IP-Adressen beschränken möchten, für die die Regel gelten soll (beispielsweise weil einer Netzwerkkarte mehrere Adressen zugewiesen wurden oder Ihr Computer über mehrere Netzwerkkarten verfügt), wählen Sie unter *Lokale IP-Adresse* die Option *Diese IP-Adressen*. Klicken Sie auf *Hinzufügen* und geben Sie die gewünschte Adresse oder Adressen an.
3. Wenn Sie die Remote-IP-Adressen beschränken möchten, für die die Regel gelten soll (weil die Regel zum Beispiel nur für den eingehenden Datenverkehr aus einem bestimmten Subnetz gelten soll), wählen Sie unter *Remote-IP-Adressen* die Option *Diese IP-Adressen* und klicken auf *Hinzufügen*, um die gewünschten IP-Adressen, Netzwerkadressen oder IP-Adressbereiche anzugeben.

Auf der Registerkarte *Erweitert* können Sie im Eigenschaftendialogfeld einer Regel festlegen, für welche Netzwerkschnittstellentypen die Regel gilt. Das ähnelt der Beschränkung der Regel auf bestimmte lokale IP-Adressen, wobei aber ein bestimmter Gerätetyp ausgewählt wird und nicht die Adresse, die diesem Gerät zugewiesen wurde. Auf der Registerkarte *Erweitert* können Sie auch festlegen, was mit dem Datenverkehr geschehen soll, der über ein Edgegerät übertragen wird, beispielsweise über einen NAT-Router (Network Address Translation, Netzwerkadressübersetzung). Folgende Optionen stehen zur Wahl:

- **Edgeausnahme blockieren** Das Ziel dieser Regel erhält über das NAT-Gerät keinen nicht angeforderten Datenverkehr aus dem Internet.
- **Edgeausnahme zulassen** Das Ziel der Regel bearbeitet den über das NAT-Gerät aus dem Internet eingegangenen nicht angeforderten Datenverkehr direkt.
- **Auf Benutzer zurückstellen** Der Benutzer wird über den Datenverkehr informiert, der über das NAT-Gerät eintrifft. Verfügt der Benutzer über die entsprechenden Rechte, kann er die Kommunikation manuell zulassen oder blockieren.
- **Auf Anwendung zurückstellen** Die Anwendungseinstellungen bestimmen, ob der über ein NAT-Gerät eintreffende Datenverkehr angenommen oder abgelehnt wird.

Verbindungssicherheitsregeln

Verbindungssicherheitsregeln sind eine spezielle Regelart für authentifizierten und verschlüsselten Datenverkehr. Mit Verbindungssicherheitsregeln können Sie festlegen, wie die Kommunikation zwischen verschiedenen Hosts im Netzwerk erfolgt. Sie erstellen diese Regeln mit dem Assistenten für neue Verbindungssicherheitsregeln (Abbildung 7.10). Verbindungen können mit dem Protokoll Kerberos V5 authentifiziert und auf Computer oder auf Computer und Benutzer beschränkt werden, die der Domäne angehören. Wenn Sie auf der Seite *Authentifizierungsmethode* des Assistenten die Option *Erweitert* wählen, können Verbindungen mit Kerberos V5, NTLMv2, mit Computerzertifikaten von einer bestimmten Zertifizierungsstelle oder mit einem vorinstallierten Schlüssel authentifiziert werden.

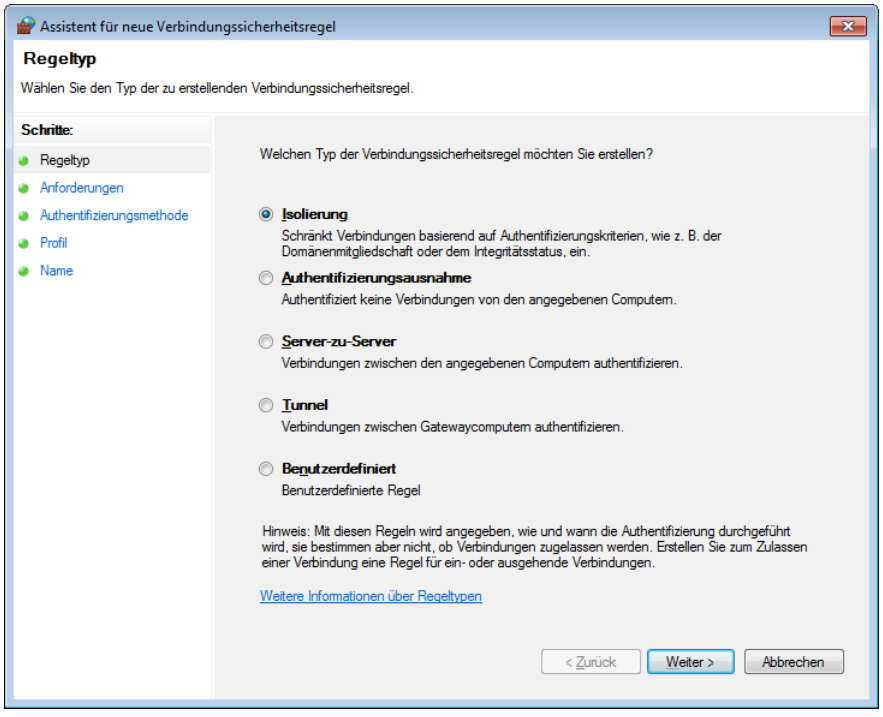

Assistent für neue Verbindungssicherheitsregel
Regeltyp
Wählen Sie den Typ der zu erstellenden Verbindungssicherheitsregel.
Schritte:
Regeltyp
Anforderungen
Authentifizierungsmethode
Profil
Name
Welchen Typ der Verbindungssicherheitsregel möchten Sie erstellen?
Isolierung
Schränkt Verbindungen basierend auf Authentifizierungskriterien, wie z. B. der Domänenmitgliedschaft oder dem Integritätsstatus, ein.
Authentifizierungsausnahme
Authentifiziert keine Verbindungen von den angegebenen Computern.
Server-zu-Server
Verbindungen zwischen den angegebenen Computern authentifizieren.
Tunnel
Verbindungen zwischen Gatewaycomputern authentifizieren.
Benutzerdefiniert
Benutzerdefinierte Regel
Hinweis: Mit diesen Regeln wird angegeben, wie und wann die Authentifizierung durchgeführt wird, sie bestimmen aber nicht, ob Verbindungen zugelassen werden. Erstellen Sie zum Zulassen einer Verbindung eine Regel für ein- oder ausgehende Verbindungen.
Weitere Informationen über Regeltypen
< Zurück
Weiter >
Abbrechen

Abbildung 7.10 Neue Verbindungssicherheitsregel

Die Verbindungssicherheitsregeln funktionieren folgendermaßen:

- **Isolierung** Isolierungsregeln ermöglichen die Beschränkung der Kommunikation auf Hosts, die sich mit bestimmten Anmeldeinformationen authentifizieren können. Mit einer Isolierungsregel können Sie zum Beispiel die Kommunikation mit Hosts sperren, die keine Mitglieder einer AD DS-Domäne (Active Directory Domain Services, Active Directory-Domänendienste) sind. Sie können die Isolierungsregel so konfigurieren, dass für eingehende und ausgehende Verbindungen eine Authentifizierung angefordert wird oder erforderlich ist, oder dass die Authentifizierung für eingehende Verbindungen erforderlich ist und für ausgehende Verbindungen angefordert wird.
- **Authentifizierungsausnahme** Diese Regel ermöglicht die Konfiguration von Ausnahmen für Isolierungsregeln. Mit Authentifizierungsausnahmen können Sie Computern zum Beispiel Verbindungen ohne Authentifizierung mit Infrastrukturservern wie DHCP-Servern und DNS-Servern ermöglichen.
- **Server-zu-Server** Mit diesen Regeln können Sie Verbindungen zwischen bestimmten Computern schützen. Sie unterscheiden sich insofern von Isolierungsregeln, als sie nicht für alle Verbindungen gelten, sondern nur für Verbindungen zwischen Hosts mit bestimmten Adressen.
- **Tunnel** Diese Regeln ähneln Server-zu-Server-Regeln, gelten aber für Verbindungen, die durch Tunnel mit Remotestandorten erfolgen, beispielsweise zur Verbindung zweier Standorte.



Hinweis Verbindungssicherheitsregeln und IPsec-Richtlinien

Die Beziehung zwischen Verbindungssicherheitsregeln und IPsec-Richtlinien ähnelt der Beziehung zwischen AppLocker und den Richtlinien für Softwareeinschränkung. Beide Regelsätze tun ähnliche Dinge, aber welcher sich verwenden lässt, hängt von den Betriebssystemen der Clientcomputer ab. Alle Editionen von Windows 7 und Windows Vista unterstützen Verbindungssicherheitsregeln, Windows XP jedoch nicht.

Importieren und Exportieren der Firewall-Konfiguration

Die meisten Organisationen, die Windows 7-Clients verwenden, wenden Firewallregeln über Gruppenrichtlinien an. Falls Sie auch einige eigenständige Windows 7-Computer unterstützen müssen, können Sie komplexe Firewallkonfigurationen mit den WFAS-Optionen *Richtlinie importieren* und *Richtlinie exportieren* übertragen. Der Export und Import der Richtlinien ermöglicht es auch, die aktuelle Firewallkonfiguration zu sichern, bevor Änderungen vorgenommen werden. Exportierte Richtliniendateien haben die Namenserweiterung *.wfw* und liegen in einem binären Format vor, also nicht wie viele andere Windows 7-Konfigurationsdateien im XML-Format (Extensible Markup Language). Mit den Befehlen `netsh advfirewall export` oder `netsh advfirewall import` können Sie Firewallrichtlinien in dasselbe *.wfw*-Format exportieren und wieder importieren.

Verwalten von WFAS mit Netsh

Sie können WFAS-Regeln auch in einer Eingabeaufforderung mit erhöhten Rechten mit dem Befehlszeilenprogramm *Netsh.exe* verwalten. Der Vorteil liegt darin, dass Sie es mit Windows-Remoteshell (WinRS) kombinieren können, worüber Sie in der nächsten Lektion mehr erfahren, um WFAS-Regeln auf anderen Windows 7-Computern Ihres Netzwerks zu verwalten. Außerdem können Sie *Netsh.exe* in Skripts zur Erstellung von Firewallregeln auf eigenständigen Computern verwenden, die nicht Mitglieder einer AD DS-Domäne sind und daher nicht mit Domänenrichtlinien gesteuert werden.

Zur Erstellung von WFAS-Firewallregeln mit *Netsh.exe* müssen Sie sich im Kontext `advfirewall firewall` befinden. Die folgenden Beispiele zeigen, wie man mit *Netsh.exe* WFAS-Firewallregeln erstellen kann:

- Zur Erstellung einer Regel namens WebServerRegel, die im Domänenprofil gilt und eingehenden Datenverkehr auf dem TCP-Port 80 zulässt, verwenden Sie den Befehl **netsh advfirewall firewall add rule name="WebServerRegel" profile=domain protocol=TCP dir=in localport=80 action=allow**.
- Zur Erstellung einer Regel namens CalcZulassen, die eingehenden Datenverkehr für die Anwendung *Calc.exe* in allen Netzwerkprofilen zulässt, verwenden Sie den Befehl **netsh advfirewall firewall add rule name="CalcZulassen" dir=in program="c:\Windows\System32\Calc.exe"**.
- Zur Erstellung einer Regel namens FTPBlockieren, die ausgehenden Datenverkehr der Anwendung *Ftp.exe* blockiert, verwenden Sie den Befehl **netsh advfirewall firewall add rule name="FTPBlockieren" dir=out program="c:\Windows\System32\ftp.exe" action=block**.



Prüfungstipp

Merken Sie sich, wann Sie WFAS zur Erstellung einer Regel verwenden müssen und wann die Windows-Firewall ausreicht.

Übung Konfigurieren der Windows-Firewall

In dieser Übung verwenden Sie die Windows-Firewall und WFAS, um zwei verschiedene Firewallregeln zu konfigurieren. Durch die Arbeit mit den Konfigurationstools erfahren Sie mehr über die Regeltypen, die Sie in jedem Tool konfigurieren können.

Übung 1 Konfigurieren von Firewallregeln mit der Windows-Firewall

In dieser Übung richten Sie eine Regel ein, die eingehenden Datenverkehr mit der Anwendung Internet Backgammon zulässt:

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Klicken Sie auf *Start*, dann auf *Systemsteuerung* und schließlich auf *System und Sicherheit*.
3. Klicken Sie unter *Windows-Firewall* auf *Programm über die Windows-Firewall kommunizieren lassen*.
4. Klicken Sie im Dialogfeld *Kommunikation von Programmen durch die Windows-Firewall zulassen* auf *Einstellungen ändern* (Abbildung 7.11).

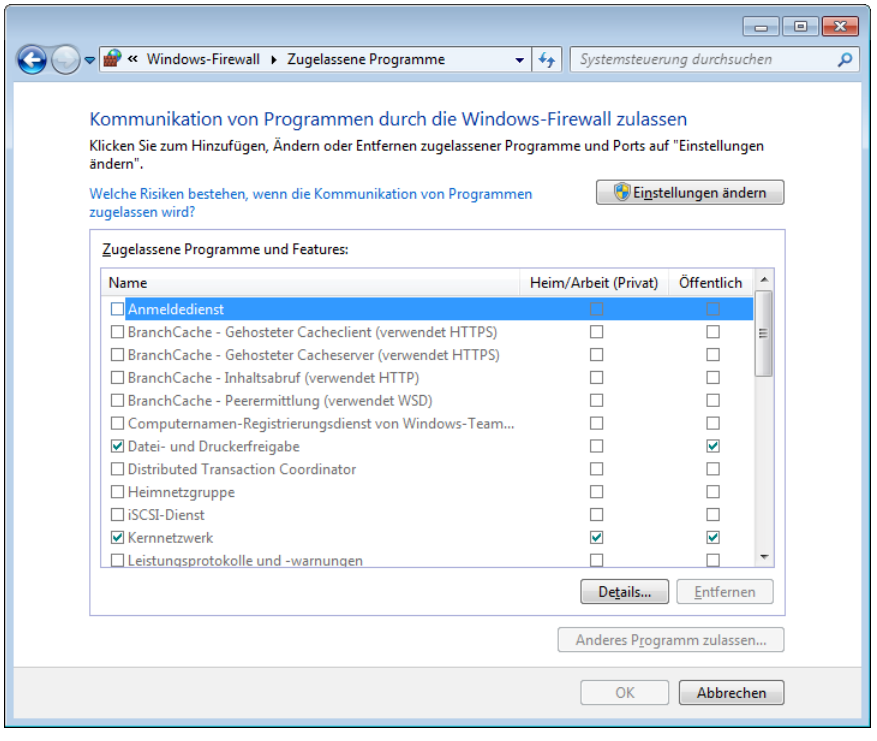


Abbildung 7.11 Zulassen von Programmen in der Windows-Firewall

5. Klicken Sie auf *Anderes Programm zulassen*. Dadurch öffnet sich das Dialogfeld *Programm hinzufügen*. Klicken Sie auf *Durchsuchen* und navigieren Sie in den Ordner *Programme\Microsoft Games\Multiplayer\Backgammon*. Wählen Sie *Bckgzm.exe* und klicken Sie auf *Öffnen*.
6. Klicken Sie auf *Netzwerkstandorttypen* und überprüfen Sie die Einstellungen anhand von Abbildung 7.12. Klicken Sie auf *OK* und dann auf *Hinzufügen*.

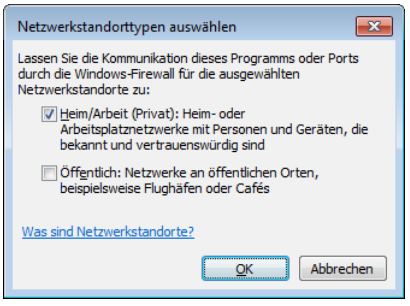

Netzwerkstandorttypen auswählen
Lassen Sie die Kommunikation dieses Programms oder Ports durch die Windows-Firewall für die ausgewählten Netzwerkstandorte zu:
Heim/Arbeit (Privat): Heim- oder Arbeitsplatznetzwerke mit Personen und Geräten, die bekannt und vertrauenswürdig sind
Öffentlich: Netzwerke an öffentlichen Orten, beispielsweise Flughäfen oder Cafés
Was sind Netzwerkstandorte?
OK
Abbrechen

Abbildung 7.12 Auswählen des Netzwerkstandorttyps

7. Überprüfen Sie, ob in der Liste *Zugelassene Programme und Features* für das Profil *Heim/Arbeit (Privat)* nun eine Regel vorhanden ist, aber nicht im Profil *Öffentlich*, und klicken Sie dann auf *OK*.

Übung 2 Konfigurieren von WFAS-Regeln

In dieser Übung richten Sie eine WFAS-Regel für einen hypothetischen IRC-Server (Internet Relay Chat) ein, der auf einem Clientcomputer unter Windows 7 betrieben wird. Sie konfigurieren eine Regel, die nur authentifizierte Verbindungen von Hosts aus einem bestimmten Subnetz zulässt.

1. Sofern Sie es noch nicht getan haben, melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* den Text **Windows-Firewall mit erweiterter Sicherheit** ein und klicken Sie auf *Windows-Firewall mit erweiterter Sicherheit*. Dadurch öffnet sich die Konsole *Windows-Firewall mit erweiterter Sicherheit*.
3. Wählen Sie den Knoten *Eingehende Regeln*. Klicken Sie im Bereich *Aktionen* auf *Neue Regel*.
4. Wählen Sie auf der Seite *Regeltyp* den Typ *Port* und klicken Sie dann auf *Weiter*.
5. Geben Sie auf der Seite *Protokoll und Ports* im Textfeld *Bestimmte lokale Ports* die Portnummer **6667** ein (Abbildung 7.13) und klicken Sie dann auf *Weiter*.
6. Wählen Sie auf der Seite *Aktion* die Option *Verbindung zulassen, wenn sie sicher ist* und klicken Sie dann auf *Anpassen*.
7. Wählen Sie im Dialogfeld *Einstellungen für das Zulassen sicherer Verbindungen anpassen* die Option *Verschlüsselung der Verbindungen erforderlich* und wählen Sie dann das Kontrollkästchen *Dynamisches Verhandeln der Verschlüsselung für Computer zulassen* (Abbildung 7.14). Klicken Sie dann auf *OK*.

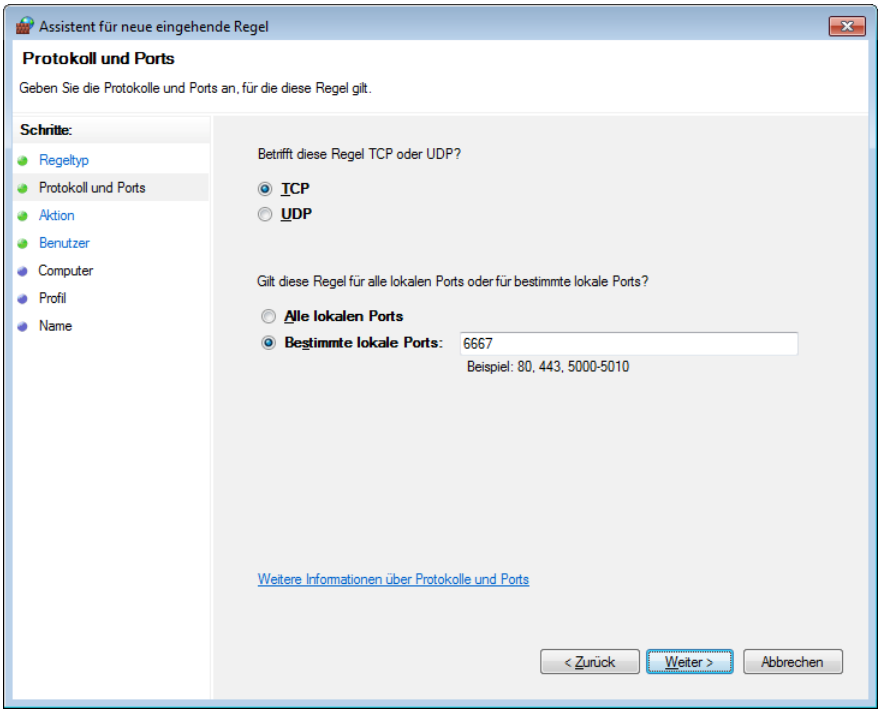


Abbildung 7.13 Angeben des TCP-Ports 6667

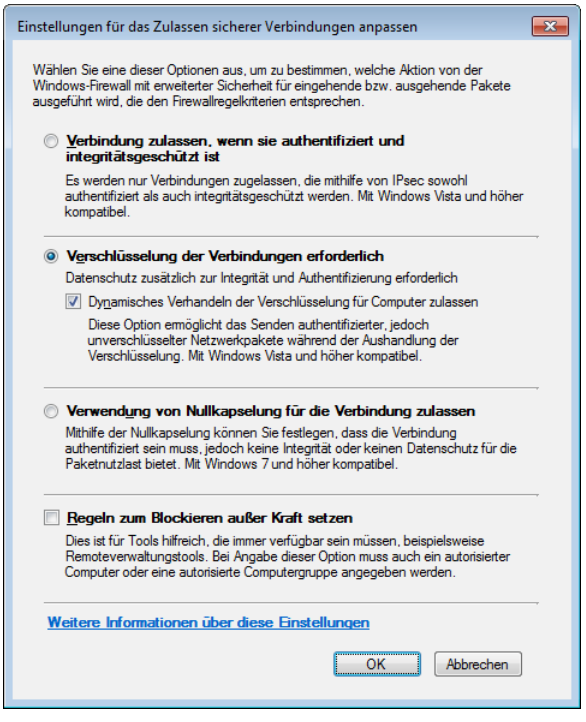

Einstellungen für das Zulassen sicherer Verbindungen anpassen
Wählen Sie eine dieser Optionen aus, um zu bestimmen, welche Aktion von der Windows-Firewall mit erweiterter Sicherheit für eingehende bzw. ausgehende Pakete ausgeführt wird, die den Firewallregelkriterien entsprechen.
Verbindung zulassen, wenn sie authentifiziert und integritätsgeschützt ist
Es werden nur Verbindungen zugelassen, die mithilfe von IPsec sowohl authentifiziert als auch integritätsgeschützt werden. Mit Windows Vista und höher kompatibel.
Verschlüsselung der Verbindungen erforderlich
Datenschutz zusätzlich zur Integrität und Authentifizierung erforderlich
Dynamisches Verhandeln der Verschlüsselung für Computer zulassen
Diese Option ermöglicht das Senden authentifizierter, jedoch unverschlüsselter Netzwerkpakete während der Aushandlung der Verschlüsselung. Mit Windows Vista und höher kompatibel.
Verwendung von Nullkapselung für die Verbindung zulassen
Mithilfe der Nullkapselung können Sie festlegen, dass die Verbindung authentifiziert sein muss, jedoch keine Integrität oder keinen Datenschutz für die Paketnutzlast bietet. Mit Windows 7 und höher kompatibel.
Regeln zum Blockieren außer Kraft setzen
Dies ist für Tools hilfreich, die immer verfügbar sein müssen, beispielsweise Remoteverwaltungstools. Bei Angabe dieser Option muss auch ein autorisierter Computer oder eine autorisierte Computergruppe angegeben werden.
Weitere Informationen über diese Einstellungen
OK
Abbrechen

Abbildung 7.14 Anpassen der Einstellungen für sichere Verbindungen

8. Klicken Sie auf *Weiter*. Klicken Sie auf der Seite *Benutzer* des Assistenten für neue eingehende Regeln ebenfalls auf *Weiter*.
9. Klicken Sie auf der Seite *Computer* des Assistenten für neue eingehende Regeln wieder auf *Weiter*.
10. Legen Sie auf der Seite *Wann wird diese Regel angewendet* fest, dass die Regel nur für die Profile *Domäne* und *Privat* gilt, und klicken Sie dann auf *Weiter*.
11. Geben Sie auf der Seite *Name* den Namen **IRC-Serverregel** ein und klicken Sie dann auf *Fertig stellen*.
12. Klicken Sie in der Liste *Eingehende Regeln* mit der rechten Maustaste die *IRC-Serverregel* an und wählen Sie dann *Eigenschaften*.
13. Klicken Sie auf die Registerkarte *Bereich*. Wählen Sie im Abschnitt *Remote-IP-Adresse* die Option *Diese IP-Adressen* und klicken Sie dann auf *Hinzufügen*.
14. Geben Sie im Textfeld *Diese IP-Adresse oder dieses Subnetz* **10.0.10.0/24** ein und klicken Sie dann auf *OK*.
15. Überprüfen Sie das Dialogfeld *Eigenschaften von IRC-Serverregel* anhand von Abbildung 7.15 und klicken Sie dann auf *OK*.

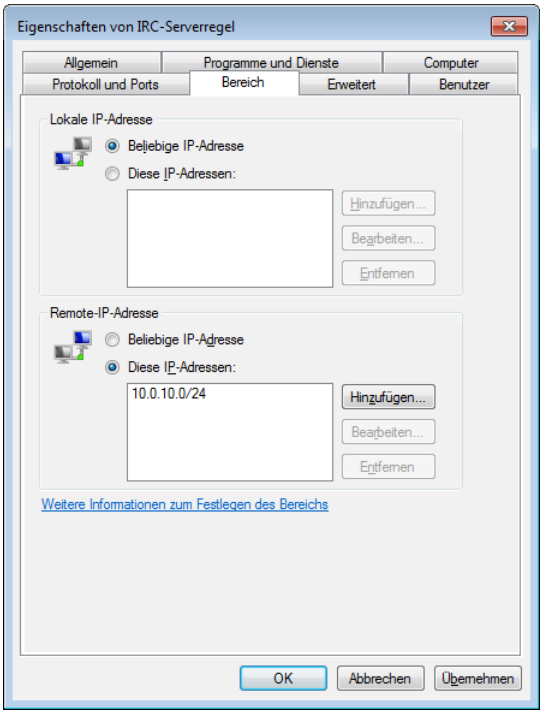


Abbildung 7.15 Konfigurieren des Regelbereichs

Zusammenfassung der Lektion

- Auf einem Clientcomputer, auf dem Windows 7 ausgeführt wird, arbeiten die Windows-Firewall und die Windows-Firewall mit erweiterter Sicherheit (Windows Firewall with Advanced Security, WFAS) zusammen.
- Die Windows-Firewall ermöglicht die Erstellung von einfachen Regeln für Programme und Windows 7-Funktionen. Sie können unter der Windows-Firewall aber beispielsweise keine Bereiche oder Authentifizierungseinstellungen konfigurieren.
- Netzwerkprofile ermöglichen die Erstellung von unterschiedlichen Regelsätzen für unterschiedliche Netzwerkstandortkategorien. Verfügbar sind die drei Netzwerkprofile *Domäne*, *Öffentlich* und *Heim oder Arbeitsplatz (privat)*.
- Windows-Firewallregeln können in den Netzwerkprofilen selektiv aktiviert werden. Für verschiedene Netzwerkkarten können gleichzeitig verschiedene Netzwerkprofile gelten.
- WFAS ermöglicht die Konfiguration von eingehenden und ausgehenden Firewallregeln für Ports, Programme und Dienste.
- WFAS ermöglicht die Konfiguration des Regelbereichs und der Authentifizierung.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Verwalten der Windows-Firewall«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie sind an einer kleinen Schule für die Verwaltung der Windows 7-Laptops zuständig. Sie möchten verhindern, dass die Schüler mit FTP Dateien auf FTP-Sites aus dem Internet hochladen können. Allerdings sollen die Schüler ausgehende E-Mails mit SMTP (Simple Mail Transfer Protocol) senden können. Welche der folgenden Regeln würden Sie konfigurieren?
   A. Eingehende Regeln
   B. Ausgehende Regeln
   C. Isolierungsregeln
   D. Authentifizierungsausnahmeregeln
2. Sie möchten eine Firewallregel erstellen, die eingehende Verbindungen auf TCP-Port 80 zulässt, wenn Ihr Windows 7-Laptop mit Ihrem Büronetzwerk verbunden ist, aber eingehende Verbindungen auf TCP-Port 80 blockiert, wenn der Laptop mit Ihrem Heimnetzwerk verbunden ist. Mit welchem der folgenden Tools können Sie diese Regel erstellen? (Wählen Sie alle zutreffenden Antworten.)

A. Windows-Firewall
B. WFAS
C. Netsh
D. Netstat

3. Was bewirkt der Befehl `netsh advfirewall firewall add rule name="Benutzerdefinierte Regel" profile=domain protocol=TCP dir=in localport=80 action=allow` in einer Eingabeaufforderung mit erhöhten Rechten?
   A. Er erstellt eine eingehende Regel, die nur im Domänenprofil gilt und den Datenverkehr auf Port 80 blockiert.
   B. Er erstellt eine ausgehende Regel, die nur im Domänenprofil gilt und den Datenverkehr auf Port 80 blockiert.
   C. Er erstellt eine eingehende Regel, die nur im Domänenprofil gilt und den Datenverkehr auf Port 80 zulässt.
   D. Er erstellt eine ausgehende Regel, die nur im Domänenprofil gilt und den Datenverkehr auf Port 80 zulässt.
4. Sie konfigurieren auf einem Windows 7-Clientcomputer Firewallregeln. Sie möchten eingehende Verbindungen mit der Anwendung *Application.exe* zulassen, aber nur wenn eine Authentifizierung erfolgt. Wie erreichen Sie dieses Ziel?
   A. Sie erstellen mit der Windows-Firewall eine Regel.
   B. Sie erstellen mit WFAS eine Regel.
   C. Sie erstellen mit der Anmeldeinformationsverwaltung eine Regel.
   D. Sie erstellen mit dem Autorisierungs-Manager eine Regel.
5. Sie möchten, dass Windows 7 Sie informiert, wenn Ihr Computer mit dem Domänennetzwerk Ihrer Organisation verbunden ist und die Firewall ein neues Programm blockiert. Windows 7 soll Sie nicht informieren, wenn Ihr Computer mit einem öffentlichen Netzwerk verbunden ist und die Firewall ein neues Programm blockiert. Welche der folgenden Einstellungen nehmen Sie vor? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)
   A. Sie wählen im Bereich *Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)* die Option *Windows-Firewall aktivieren* und aktivieren das Kontrollkästchen *Benachrichtigen, wenn ein neues Programm blockiert wird*.
   B. Sie wählen im Bereich *Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)* die Option *Windows-Firewall aktivieren* und deaktivieren das Kontrollkästchen *Benachrichtigen, wenn ein neues Programm blockiert wird*.
   C. Sie wählen im Bereich *Standorteinstellungen für das öffentliche Netzwerk* die Option *Windows-Firewall aktivieren* und aktivieren das Kontrollkästchen *Benachrichtigen, wenn ein neues Programm blockiert wird*.
   D. Sie wählen im Bereich *Standorteinstellungen für das öffentliche Netzwerk* die Option *Windows-Firewall aktivieren* und deaktivieren das Kontrollkästchen *Benachrichtigen, wenn ein neues Programm blockiert wird*.

Lektion 2: Windows 7-Remoteverwaltung

Die Remoteverwaltung ermöglicht es einem Benutzer, Verwaltungsarbeiten auf einem Computer auszuführen, der sich an einem anderen Ort befindet. Über die Remoteverwaltung können Sie fast jede Aufgabe remote erledigen, die Sie auch erledigen könnten, wenn Sie direkt vor dem Computer sitzen. In dieser Lektion erfahren Sie etwas über die Remoteverwaltungstechnologien, die Sie unter Windows 7 verwenden können, wie Remotedesktop, Remoteunterstützung, Windows PowerShell und Windows-Remoteshell (WinRS).

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Verwenden von Windows PowerShell zur Remoteverwaltung
- Verwenden von WinRS zur Remoteverwaltung
- Konfigurieren der Remoteunterstützung
- Konfigurieren von Remotedesktop

Veranschlagte Zeit für diese Lektion: 40 Minuten

Remotedesktop

Remotedesktop ermöglicht es Ihnen, sich auf einem Windows 7-Remotecomputer anzumelden und so mit dem Computer zu arbeiten, als würden Sie direkt vor dem Computer sitzen. Remotedesktop ermöglicht zum Beispiel den Druck auf Druckern, die am Remotecomputer angeschlossen sind. Sie können auch mit einer Anwendung, die auf dem Remotecomputer ausgeführt wird, auf einem lokalen Drucker drucken. Als Verwaltungstool eignet sich Remotedesktop sehr gut, weil es den Leuten, die für die Verwaltung, Wartung und Konfiguration von Clientbetriebssystemen zuständig sind, ermöglicht, viele dieser Arbeiten remote auszuführen.



Hinweis Remoteverwaltungsterminologie

Mit dem Verwaltungscomputer ist in dieser Lektion der Computer gemeint, an dem der Benutzer direkt angemeldet ist. Der Remotecomputer ist der Computer, mit dem der Benutzer eine Remotedesktopverbindung herstellt. Alle Remoteverwaltungstechnologien setzen eine Netzwerkverbindung zwischen dem Verwaltungscomputer und dem Remotecomputer voraus.

Sie können sich mit Remotedesktop an einem Computer anmelden, wenn kein anderer am Remotecomputer angemeldet ist. Allerdings muss der Computer eingeschaltet und hochgefahren sein. Wenn die physische Netzwerkkarte des Remotecomputers so konfiguriert ist, dass sie eine Aktivierung durch das LAN (Local Area Network) zulässt, kann der Computer beim Eingang einer Remotedesktopverbindungsaufforderung aus einem Ruhezustand reaktiviert werden. Allerdings geht die Konfiguration von Windows 7 für diese Arbeitsweise über den Stoff der Prüfung 70-680 hinaus. Wenn ein Benutzer die interaktive Sitzung auf seinem Windows 7-Computer sperrt, kann er eine Remoteverbindung mit diesem Computer herstellen und die Sitzung über Remotedesktop fortführen. Außerdem kann er die Verbindung mit dieser Sitzung trennen und die Sitzung weiterführen, wenn er sich wieder direkt am Computer anmeldet.

Wenn bereits ein anderer Benutzer am Computer angemeldet ist und eine eingehende Remotedesktopsitzung eingeleitet wird, erhält er die Meldung, dass sich ein anderer Benutzer remote anmelden möchte (Abbildung 7.16). Der angemeldete Benutzer hat nun die Möglichkeit, den Remotezugriff auch dann abzulehnen, wenn der Remotebenutzer über Administratorrechte verfügt und der direkt angemeldete Benutzer nicht.

Wenn ein Benutzer remote angemeldet ist und ein anderer Benutzer versucht, sich vor Ort anzumelden, wird der Remotebenutzer in gleicher Weise informiert. Der angemeldete Benutzer hat unabhängig davon, ob er lokal oder remote angemeldet ist, immer die Möglichkeit, die Anmeldung eines anderen Benutzers abzulehnen. Wird ein Benutzer getrennt, bleibt seine Sitzung im Speicher und er kann später wieder eine Verbindung mit der Sitzung herstellen. Das funktioniert so ähnlich wie beim schnellen Benutzerwechsel über das Startmenü, bei dem die aktuelle Sitzung erhalten bleibt und später weitergeführt werden kann.

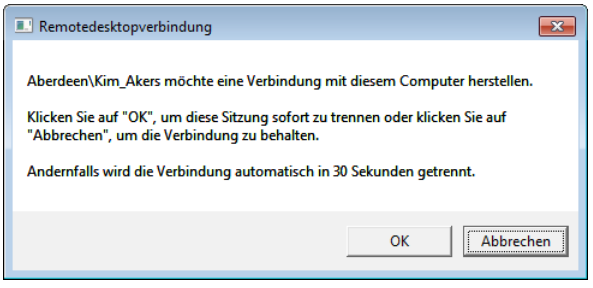

Remotedesktopverbindung
Aberdeen\Kim_Akers möchte eine Verbindung mit diesem Computer herstellen.
Klicken Sie auf "OK", um diese Sitzung sofort zu trennen oder klicken Sie auf "Abbrechen", um die Verbindung zu behalten.
Andernfalls wird die Verbindung automatisch in 30 Sekunden getrennt.
OK
Abbrechen

Abbildung 7.16 Der angemeldete Benutzer kann eine Remotedesktopverbindung ablehnen

Sie können über NAT-Geräte Remotedesktopverbindungen mit Hosts aus dem Internet herstellen. Eine in Windows Server 2008 verfügbare Technologie namens Terminaldienstegateway ermöglicht es Benutzern, Remotedesktopverbindungen von Hosts, die über eine Internetverbindung verfügen, mit Hosts aus einem internen geschützten Netzwerk herzustellen. Remotedesktopverbindungen lassen sich über Modem und VPN-Verbindungen herstellen. Außerdem können Remotedesktopverbindungen die Protokolle IPv4 und IPv6 verwenden, und es ist auch möglich, eine Remotedesktopverbindung herzustellen, wenn ein Computer mit DirectAccess eine Verbindung mit dem Netzwerk herstellt.

Konfigurieren von Remotedesktop

Remotedesktopverbindungen lassen sich nur auf Computern herstellen, auf denen die Editionen Professional, Enterprise oder Ultimate von Windows 7 verwendet werden. Andere Windows 7-Editionen unterstützen zwar keine eingehenden Remotedesktopverbindungen, aber alle Editionen enthalten die Remotedesktop-Clientsoftware. Remotedesktop wird unter Windows 7 nicht standardmäßig aktiviert. Sie können es auf der Registerkarte *Remote* des Dialogfelds *Systemeigenschaften* aktivieren (Abbildung 7.17). Bei der Aktivierung von Remotedesktop können Sie Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird, oder die Verbindungen auf Computer beschränken, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird. Nur Windows Vista- und Windows 7-Clients unterstützen standardmäßig eine Authentifizierung auf Netzwerkebene. Es ist zwar auch möglich, Computer, auf denen Windows XP mit SP3 verwendet wird, für eine Authentifizierung auf Netzwerkebene zu konfigurieren,

aber diese Funktion wird nicht standardmäßig unterstützt. Wenn Sie von einem Windows XP-Client ohne SP3 aus eine Verbindung mit einem Windows 7-Client herstellen wollen, müssen Sie die Option wählen, mit der Verbindungen von beliebigen Versionen von Remotedesktop zugelassen werden.

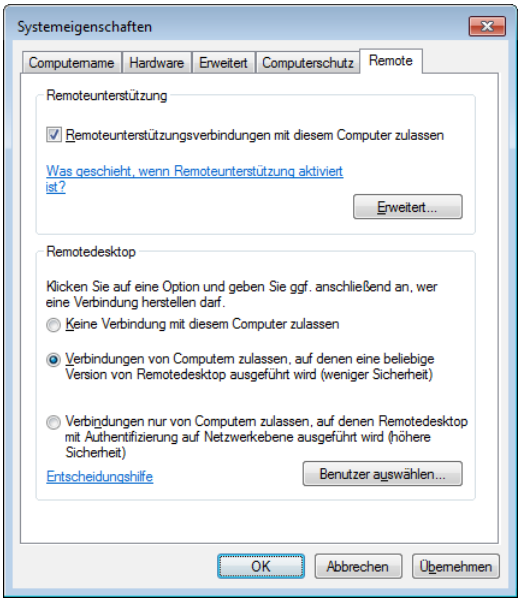

Systemeigenschaften
Computername
Hardware
Erweitert
Computerschutz
Remote
Remoteunterstützung
Remoteunterstützungsverbindungen mit diesem Computer zulassen
Was geschieht, wenn Remoteunterstützung aktiviert ist?
Erweitert...
Remotedesktop
Klicken Sie auf eine Option und geben Sie ggf. anschließend an, wer eine Verbindung herstellen darf.
Keine Verbindung mit diesem Computer zulassen
Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird (weniger Sicherheit)
Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird (höhere Sicherheit)
Entscheidungshilfe
Benutzer auswählen...
OK
Abbrechen
Übernehmen

Abbildung 7.17 Aktivieren von Remotedesktop

Wenn Sie Remotedesktop aktivieren, aktualisiert die Windows-Firewall automatisch die Regeln, um Remotedesktopverbindungen mit dem Computer zuzulassen. Sofern Sie die Windows-Firewall anschließend auf die Standardeinstellungen zurücksetzen, müssen Sie die Remotedesktopregeln manuell wieder aktivieren. Sie können diese Regeln allerdings auch wieder aktivieren, indem Sie Remotedesktop erst deaktivieren und dann wieder aktivieren.

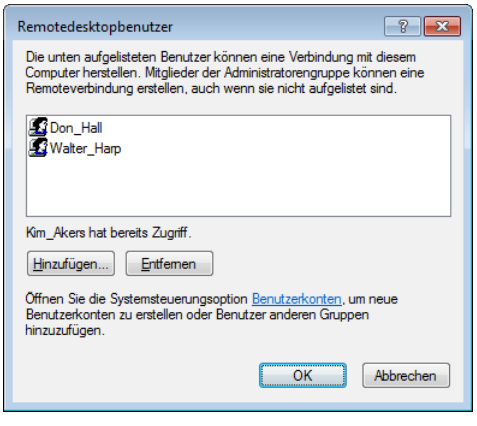

Remotedesktopbenutzer
Die unten aufgelisteten Benutzer können eine Verbindung mit diesem Computer herstellen. Mitglieder der Administratorengruppe können eine Remoteverbindung erstellen, auch wenn sie nicht aufgelistet sind.
Don_Hall
Walter_Harp
Kim_Akers hat bereits Zugriff.
Hinzufügen...
Entfernen
Öffnen Sie die Systemsteuerungsoption Benutzerkonten, um neue Benutzerkonten zu erstellen oder Benutzer anderen Gruppen hinzuzufügen.
OK
Abbrechen

Abbildung 7.18 Remotedesktopbenutzer

Wenn Sie einem Standardbenutzer die Erstellung von Remoteverbindungen mit Remotedesktop ermöglichen wollen, müssen Sie sein Konto zur lokalen Gruppe *Remotedesktopbenutzer* hinzufügen. Nur Mitglieder der lokalen Gruppen *Administratoren* und *Remotedesktopbenutzer* können mit Remotedesktop eine Verbindung mit einem Windows 7-Client herstellen. Wenn Sie auf der Registerkarte *Remote* des Dialogfelds *Systemeigenschaften* auf die Schaltfläche *Benutzer auswählen* klicken, öffnet sich das Dialogfeld *Remotedesktopbenutzer* (Abbildung 7.18). Jeder Benutzer, den Sie in diesem Dialogfeld hinzufügen, wird automatisch ein Mitglied der Gruppe *Remotedesktopbenutzer*. Die Liste zeigt alle Mitglieder dieser Gruppe an, unabhängig von der Methode, mit der die Benutzerkonten zu der Gruppe hinzugefügt wurden.

In einer Übung am Ende dieser Lektion konfigurieren Sie Remotedesktop.

Remoteunterstützung

Remoteunterstützung und Remotedesktop ermöglichen es dem Benutzer am Verwaltungscomputer, den Desktop und die Anwendungen des Remotecomputers zu sehen. Der Unterschied zwischen Windows-Remoteunterstützung und Remotedesktop liegt darin, dass bei der Remoteunterstützung ein Benutzer am Remotecomputer sitzt und die Remoteunterstützungssitzung einleitet, während eine Remotedesktopsitzung am Verwaltungscomputer eingeleitet wird. Remoteunterstützung ist ein Supporttool, mit dem Mitarbeiter der Supportabteilung den Bildschirm der Person, die sie beraten, praktisch so sehen können, wie ihn diese Person vor Augen hat. Dank der Remoteunterstützung müssen technisch weniger geschulte Mitarbeiter das Problem, das sie mit dem Computer haben, nicht mehr so genau beschreiben, weil die Supportmitarbeiter den Desktop direkt sehen können. Im Gegensatz zu Windows XP enthält die Remoteunterstützung von Windows 7 aber keinen Sprachclient mehr. Wenn Sie mit der Person sprechen möchten, der Sie per Remoteunterstützung helfen, brauchen Sie einen anderen Kommunikationsweg, beispielsweise ein Telefon.

Remoteunterstützung kann nur mit dem Einverständnis der Person verwendet werden, die am Remotecomputer angemeldet ist. Einladungen zur Remoteunterstützung haben nur eine beschränkte Gültigkeitsdauer. Nach dem Schließen der Remoteunterstützungsanwendung ist es nicht möglich, über eine Remoteunterstützungssitzung wieder eine Verbindung mit dem Remotecomputer herzustellen. Die Person, die am Remotecomputer angemeldet ist, kann die Remoteunterstützungssitzung jederzeit beenden. Die Standardeinstellung der Remoteunterstützung ermöglicht dem Helfer nur, den Desktop des Remotecomputers zu sehen. Er kann aber die Möglichkeit zur direkten Interaktion anfordern (Abbildung 7.19). Das ist nützlich, wenn der Helfer auf die Meldungen der Benutzerkontensteuerung reagieren muss. Die Person, die Hilfe angefordert hat, kann die Freigabe der Steuerung mit einem Klick auf die Schaltfläche *Freigabe beenden* des Programms Windows-Remoteunterstützung beenden und zur reinen Anzeige zurückkehren. Mit einem Klick auf die Schaltfläche *Anhalten* kann sie den Desktop temporär ausblenden, damit der Helfer ihn nicht sieht.

Wie Remotedesktopverbindungen kommen auch Remoteunterstützungsverbindungen nur zustande, wenn eine funktionierende Kommunikationsverbindung zwischen dem Verwaltungscomputer und dem Remotecomputer besteht. Netzwerkprobleme lassen sich mit der Remoteunterstützung also nicht beheben, weil diese Verbindungsprobleme wahrscheinlich verhindern, dass eine Remoteunterstützungssitzung zustande kommt. Die Windows-Remoteunterstützungsregel in der Windows-Firewall wird automatisch aktiviert, wenn die Windows-Remoteunterstützung auf einem Computer aktiviert wird.

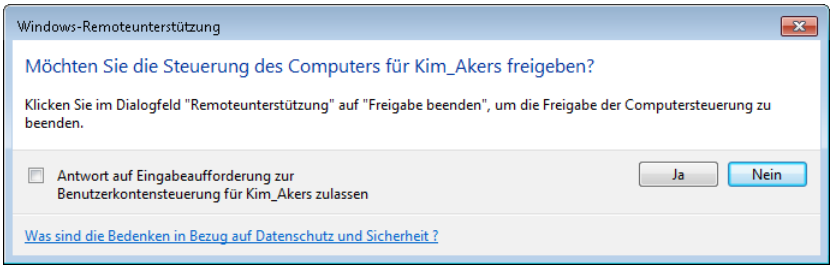

Windows-Remoteunterstützung
Möchten Sie die Steuerung des Computers für Kim_Akers freigeben?
Klicken Sie im Dialogfeld "Remoteunterstützung" auf "Freigabe beenden", um die Freigabe der Computersteuerung zu beenden.
Antwort auf Eingabeaufforderung zur Benutzerkontensteuerung für Kim_Akers zulassen
Ja
Nein
Was sind die Bedenken in Bezug auf Datenschutz und Sicherheit ?

Abbildung 7.19 Freigeben der Steuerung

Sie aktivieren die Windows-Remoteunterstützung auf der Registerkarte *Remote* des Dialogfelds *Systemeigenschaften*. Auf Windows 7-Computern wird die Windows-Remoteunterstützung standardmäßig aktiviert. In den erweiterten Remoteunterstützungseinstellungen, die nach einem Klick auf die Schaltfläche *Erweitert* der Registerkarte *Remote* des Dialogfelds *Systemeigenschaften* zugänglich sind, können Sie die Gültigkeitsdauer der Einladungen festlegen und die Remoteunterstützung so einschränken, dass nur Verbindungen von Computern hergestellt werden können, auf denen Windows Vista oder höher verwendet wird (Abbildung 7.20).

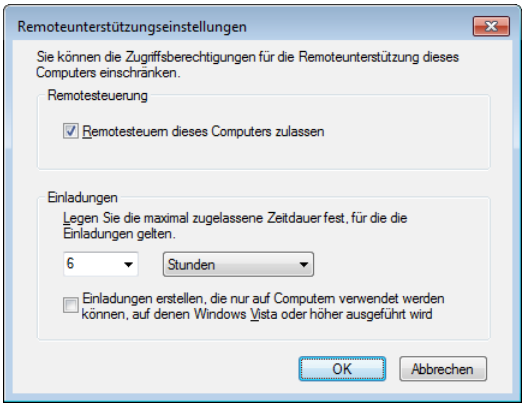

Remoteunterstützungseinstellungen
Sie können die Zugriffsberechtigungen für die Remoteunterstützung dieses Computers einschränken.
Remotesteuerung
Remotesteuern dieses Computers zulassen
Einladungen
Legen Sie die maximal zugelassene Zeitdauer fest, für die die Einladungen gelten.
6
Stunden
Einladungen erstellen, die nur auf Computern verwendet werden können, auf denen Windows Vista oder höher ausgeführt wird
OK
Abbrechen

Abbildung 7.20 Erweiterte Remoteunterstützungseinstellungen

Wenn Sie das Programm Windows-Remoteunterstützung starten, haben Sie die Wahl, eine Einladung zur Unterstützung zu erstellen oder auf eine Einladung zu reagieren (Abbildung 7.21). Wählt ein Benutzer, der Hilfe anfordern möchte, die Option *Eine vertrauenswürdige Person zur Unterstützung einladen*, hat er drei Möglichkeiten: Speichern der Einladung als Datei, Versenden der Einladung in einer E-Mail oder Verwenden von Easy Connect. Die E-Mail-Option steht nur zur Verfügung, wenn auf dem Windows 7-Client ein kompatibles E-Mail-Programm installiert ist. Im Gegensatz zu älteren Windows-Versionen wird Windows 7 aber ohne E-Mail-Programm ausgeliefert, Sie können also nicht davon ausgehen, dass ein entsprechendes Programm vorhanden ist. Die Easy Connect-Methode können Sie nur im lokalen Netzwerk verwenden, wenn auf einem lokalen Server Windows Server 2008 verwendet wird und das Peer Name Resolution-Protokoll verfügbar ist, oder wenn Sie mit Easy Connect über das Internet Hilfe anfordern und Ihr Router dieses Protokoll

unterstützt. Mit Easy Connect können Sie eine Unterstützungsanforderung versenden, ohne eine Einladung weiterleiten zu müssen.

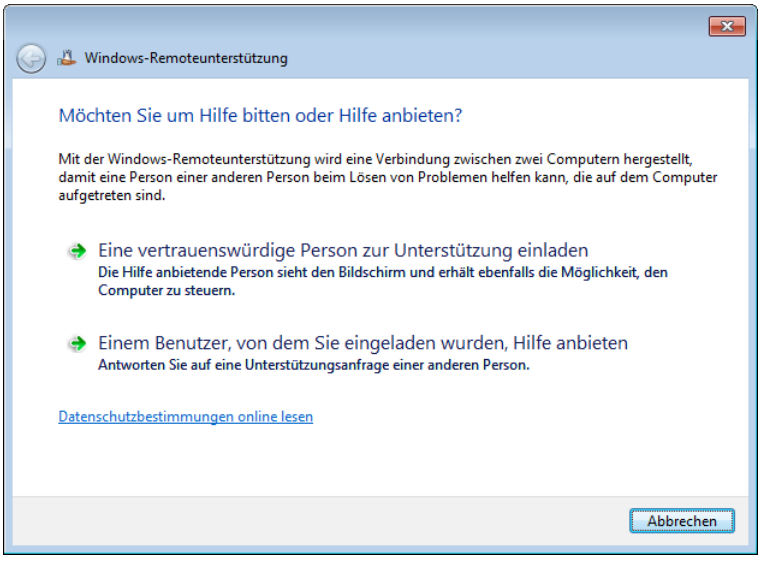

Windows-Remoteunterstützung
Möchten Sie um Hilfe bitten oder Hilfe anbieten?
Mit der Windows-Remoteunterstützung wird eine Verbindung zwischen zwei Computern hergestellt, damit eine Person einer anderen Person beim Lösen von Problemen helfen kann, die auf dem Computer aufgetreten sind.
Eine vertrauenswürdige Person zur Unterstützung einladen
Die Hilfe anbietende Person sieht den Bildschirm und erhält ebenfalls die Möglichkeit, den Computer zu steuern.
Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten
Antworten Sie auf eine Unterstützungsanfrage einer anderen Person.
Datenschutzbestimmungen online lesen
Abbrechen

Abbildung 7.21 Anfordern oder Anbieten von Remoteunterstützung

Der Helfer braucht nicht nur eine Einladung, sondern auch ein Kennwort, das er nur von der Person erhalten kann, die Hilfe anfordert (Abbildung 7.22). Aus Sicherheitsgründen sollte dieses Kennwort auf einem anderen Weg als die Einladung übermittelt werden. Wenn der Benutzer, der Hilfe anfordert, das Dialogfeld *Windows-Remoteunterstützung* schließt, kann der Remotebenutzer keine Verbindung mehr herstellen, selbst wenn die Einladung noch nicht abgelaufen ist. Nach dem Schließen des Dialogfelds muss die Windows-Remoteunterstützung neu gestartet und eine neue Einladung versendet werden, weil die alte nicht mehr gilt.

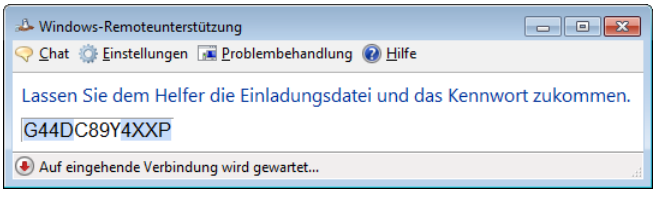


Abbildung 7.22 Warten auf eine Verbindung

Wenn der Benutzer, der um Unterstützung gebeten wurde, mit dem Kennwort, das er erhalten hat, eine Verbindung herstellt, erhält der Hilfesuchende den Hinweis, dass der Helfer alles sehen kann, was sich auf dem Desktop befindet (Abbildung 7.23). Nimmt der Hilfesuchende die Verbindung an, beginnt die Windows-Remoteunterstützungssitzung. Die Sitzung kann von beiden Beteiligten jederzeit beendet werden.

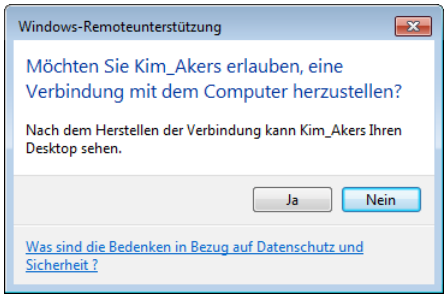

Windows-Remoteunterstützung
Möchten Sie Kim_Akers erlauben, eine Verbindung mit dem Computer herzustellen?
Nach dem Herstellen der Verbindung kann Kim_Akers Ihren Desktop sehen.
Ja
Nein
Was sind die Bedenken in Bezug auf Datenschutz und Sicherheit ?

Abbildung 7.23 Genehmigen der Remoteunterstützungsverbindung

Schnelltest

1. Welche Einstellung ist erforderlich, damit Remotedesktopverbindungen von Computern zulässig sind, auf denen Windows XP Professional SP2 ausgeführt wird?
2. Welches Protokoll muss auf lokalen Windows Server 2008-Computern verfügbar sein, wenn Sie in einer LAN-Umgebung Einladungen zur Windows-Remoteunterstützung mit Easy Connect weiterleiten?

Antworten zum Schnelltest

1. Sie müssen die Remotedesktopoption *Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird* wählen, statt die Zulassung auf Computer zu beschränken, die Remotedesktop mit einer Authentifizierung auf Netzwerkebene verwenden.
2. Unter Windows Server 2008 muss das Feature *Peer Name Resolution-Protokoll* installiert sein, damit Windows 7-Clients im LAN Easy Connect verwenden können.

Windows-Remoteverwaltungsdienst

Der Windows-Remoteverwaltungsdienst ermöglicht Ihnen die Ausführung von Befehlen auf einem Remotecomputer, sei es in einer herkömmlichen Eingabeaufforderung mit WinRS oder mit Windows PowerShell. Bevor Sie WinRS oder Windows PowerShell zur Remoteverwaltung verwenden können, müssen Sie den Zielcomputer mit dem Befehl WinRM konfigurieren. Dazu verwenden Sie auf dem Zielcomputer in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `WinRM quickconfig`. Die Ausführung von `WinRM quickconfig` bewirkt Folgendes:

- Der WinRM-Dienst wird gestartet.
- Der Starttyp des WinRM-Dienstes wird auf einen verzögerten automatischen Start eingestellt.
- Die Richtlinie *LocalAccountTokenFilterPolicy* wird so konfiguriert, dass lokalen Benutzern Remoteadministratorrechte gewährt werden.
- Auf *http://** wird ein WinRM-Listener konfiguriert, um WS-Verwaltungsanforderungen anzunehmen.
- Die WinRM-Firewallausnahme wird konfiguriert.

Wenn Sie versuchen, einen Remotecomputer zu verwalten, der nicht Mitglied derselben AD DS-Domäne wie der Verwaltungscomputer ist, müssen Sie den Verwaltungscomputer vielleicht so konfigurieren, dass er dem Remotecomputer vertraut. Das ist aber nur erforderlich, wenn Sie nicht HTTPS (Hypertext Protocol Secure) oder Kerberos zur Authentifizierung der Identität des Remotecomputers verwenden. Dieses Vertrauen müssen Sie wegen der bidirektionalen Natur des Remoteverwaltungsdatenverkehrs und wegen der Tatsache konfigurieren, dass zur Authentifizierung Anmeldeinformationen an den Remotecomputer weitergeleitet werden. Sie können das Vertrauen mit folgendem Befehl konfigurieren:

```
winrm set winrm/config/client @{TrustedHosts="<Name oder IP-Adresse des Remotecomputers>"}
```

Die Windows-Remoteverwaltung lässt sich auch über Gruppenrichtlinien konfigurieren. Die entsprechenden Richtlinien stehen im Knoten *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows-Remoteverwaltung* und wurden in die beiden Gruppen *WinRM-Client* und *WinRM-Dienst* aufgeteilt. Diese Richtlinien umfassen Authentifizierungseinstellungen und vertrauenswürdige Hosts.

Remoteverwaltung mit Windows-Remoteshell

Sie können WinRS (Windows Remote Shell) verwenden, um Befehlszeilenprogramme oder Skripts auf einem Remotecomputer auszuführen. Wenn Sie mit WinRS arbeiten möchten, öffnen Sie eine Eingabeaufforderung und schreiben vor den Befehl, der auf dem Remotecomputer ausgeführt werden soll, den Zusatz `WinRS -r:<RemoteComputerName>`. Soll beispielsweise auf dem Computer *Aberdeen* der Befehl Ipconfig ausgeführt werden, verwenden Sie den Befehl:

```
WinRS -r:Aberdeen ipconfig
```

Befindet sich der Computer im lokalen Netzwerk, können Sie seinen NetBIOS-Namen verwenden. Wenn er zu einem Remotenetzwerk gehört, müssen Sie vielleicht seinen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) angeben. Es ist auch möglich, Anmeldeinformationen anzugeben, die auf dem Remotecomputer verwendet werden. Wollen Sie zum Beispiel auf dem Computer *Aberdeen.contoso.internal* mit dem Benutzerkonto *Kim_Akers* den Befehl `net accounts` verwenden, der Informationen über die Kennwortrichtlinien anzeigt, verwenden Sie folgenden Befehl:

```
WinRS -r:http://aberdeen.contoso.internal -u:Kim_Akers net accounts
```

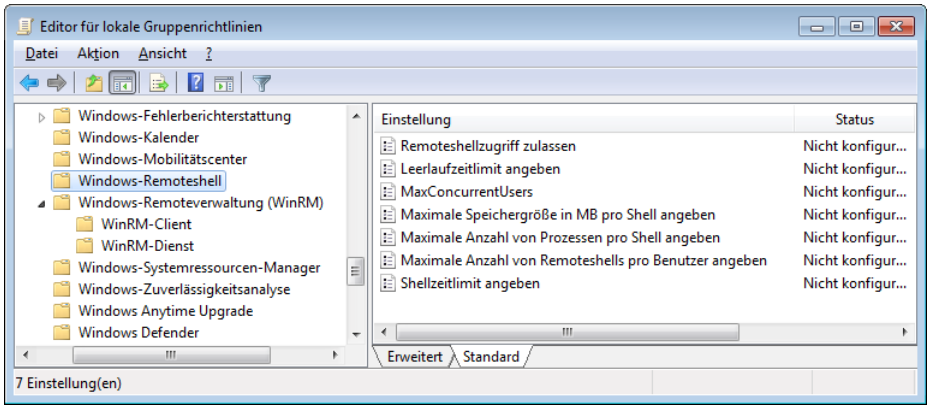


Abbildung 7.24 WinRS-Richtlinien

Wenn Sie nicht die Option `-p:<Kennwort>` verwenden, um das Kennwort anzugeben, werden Sie nach der Eingabe des Befehls zur Eingabe des Kennworts aufgefordert. Sie können die WinRS-Optionen in den Gruppenrichtlinien konfigurieren, wo sie im Knoten *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows-Remoteshell* zu finden sind (Abbildung 7.24). Mit ihnen können Sie beispielsweise Leerlaufzeitlimits oder die maximale Anzahl von Remoteshells pro Benutzer angeben oder festlegen, ob der Remoteshellzugriff zugelassen wird. In einer Übung am Ende dieser Lektion konfigurieren und verwenden Sie Windows-Remoteshell.

Remoteverwaltung mit Windows PowerShell

Windows PowerShell V2 unterstützt die Remoteverwaltung von Computern. In Windows 7 ist die Version 2.0 von Windows PowerShell enthalten. Wenn Sie einen Computer, auf dem eine ältere Windows-Version ausgeführt wird, zur Verwaltung von Windows 7 mit Windows PowerShell verwenden möchten, müssen Sie ihn auf Windows PowerShell V2 oder höher aktualisieren. Windows PowerShell können Sie nur dann zur Remoteverwaltung eines Computers verwenden, wenn Sie den Windows-Remoteverwaltungsdienst konfiguriert haben, wie in dieser Lektion bereits beschrieben. Die Syntax der Windows PowerShell-Befehle für Remotecomputer ist sehr einfach:

```
Icm Hostname {PowerShell-Befehl}
```

In einer der Übungen am Ende dieser Lektion verwenden Sie Windows PowerShell zur Remoteverwaltung.



Weitere Informationen Remoteverwaltung mit Windows PowerShell

Weitere Informationen über die Remoteverwaltung von Computern mit Windows PowerShell finden Sie in folgendem Beitrag aus dem Windows PowerShell-Blog: *http://blogs.msdn.com/powershell/archive/2008/05/10/remoting-with-powershell-quickstart.aspx.*



Prüfungstipp

Merken Sie sich, welchen Befehl Sie auf einem Computer verwenden müssen, um den Remoteverwaltungsdienst so zu konfigurieren, dass eine Remoteverwaltung mit Windows PowerShell oder WinRS möglich ist.

Übung Windows 7-Remoteverwaltungsoptionen

In dieser Übung untersuchen Sie zwei verschiedene Methoden zur Remoteverwaltung, mit denen Sie Windows 7-Computer konfigurieren und warten können. Diese Methoden ergänzen sich gegenseitig, haben aber in unterschiedlichen Situationen unterschiedliche Vorteile. Beispielsweise können Sie eine Windows PowerShell-Remotesitzung verwenden, um Informationen über einen Computer zu sammeln, während ein Benutzer angemeldet ist, oder eine Remotedesktopsitzung, wenn es um die Aktualisierung eines Treibers geht.

Übung 1 Verwenden von Remotedesktop zur Remoteverwaltung

In dieser Übung richten Sie einen Windows 7-Clientcomputer so ein, dass Remotedesktopverbindungen mit diesem Client möglich sind. Dann stellen Sie mit Remotedesktop eine Verbindung mit diesem Client her, um zu überprüfen, ob die Konfiguration korrekt ist.

1. Sorgen Sie dafür, dass der Computer *Canberra* eingeschaltet ist.
2. Schalten Sie den Computer *Aberdeen* ein und melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf diesem Computer an.
3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Überprüfen Sie mit dem Befehl `ping Canberra`, ob eine Netzwerkverbindung zwischen den Computern *Canberra* und *Aberdeen* existiert (Abbildung 7.25). Falls keine Verbindung zustande kommt, geben Sie auf beiden Computern in einer Eingabeaufforderung mit erhöhten Rechten folgende Befehle ein::
   - `netsh advfirewall firewall add rule name="ICMPv4" protocol=icmpv4:any,any dir=in action=allow`
   - `netsh advfirewall firewall add rule name="ICMPv6" protocol=icmpv6:any,any dir=in action=allow`

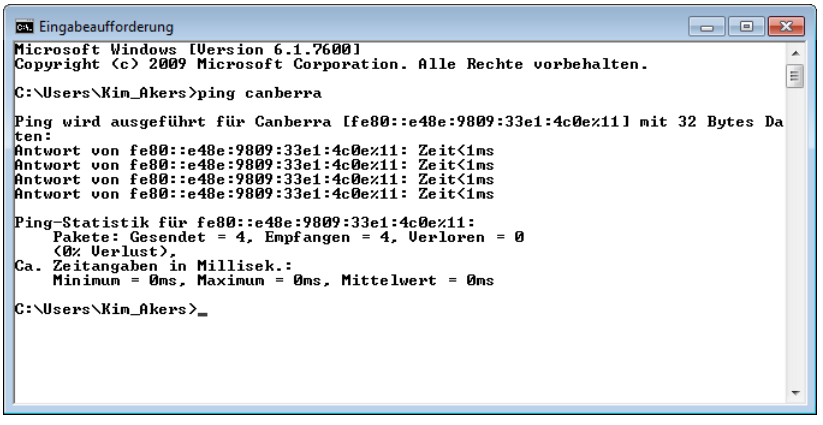

Eingabeaufforderung
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\Kim_Akers>ping canberra
Ping wird ausgeführt für Canberra [fe80::e48e:9809:33e1:4c0e%11] mit 32 Bytes Daten:
Antwort von fe80::e48e:9809:33e1:4c0e%11: Zeit<1ms
Antwort von fe80::e48e:9809:33e1:4c0e%11: Zeit<1ms
Antwort von fe80::e48e:9809:33e1:4c0e%11: Zeit<1ms
Antwort von fe80::e48e:9809:33e1:4c0e%11: Zeit<1ms
Ping-Statistik für fe80::e48e:9809:33e1:4c0e%11:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
C:\Users\Kim_Akers>

Abbildung 7.25 Überprüfen der Verbindung

4. Öffnen Sie die Systemsteuerung und klicken Sie auf *Benutzerkonten hinzufügen/entfernen*. Klicken Sie auf *Neues Konto erstellen*. Geben Sie **Cassie_Hicks** als Kontonamen für einen Standardbenutzer ein und klicken Sie auf *Konto erstellen*.
5. Klicken Sie auf der Seite *Zu änderndes Konto auswählen* auf *Cassie_Hicks*.
6. Klicken Sie auf der Seite *Änderungen am Konto von Cassie_Hicks durchführen* auf *Kennwort erstellen*. Geben Sie zweimal das Kennwort **P@ssw0rd** ein und im Textfeld *Kennworthinweis eingeben* die Nummer der Seite dieses Buchs. Klicken Sie auf *Kennwort erstellen*. Schließen Sie das Dialogfeld *Konto ändern*.
7. Klicken Sie auf *Start*. Klicken Sie *Computer* mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Klicken Sie im Bereich *Startseite der Systemsteuerung* auf *Remoteeinstellungen*.
8. Wählen Sie auf der Registerkarte *Remote* des Dialogfelds *Systemeigenschaften* die Option *Verbindungen nur von Computern zulassen, die Remotedesktop mit Authentifizierung auf Netzwerkebene verwenden (höhere Sicherheit)*, wie in Abbildung 7.26 gezeigt, und klicken Sie dann auf *Benutzer auswählen*.

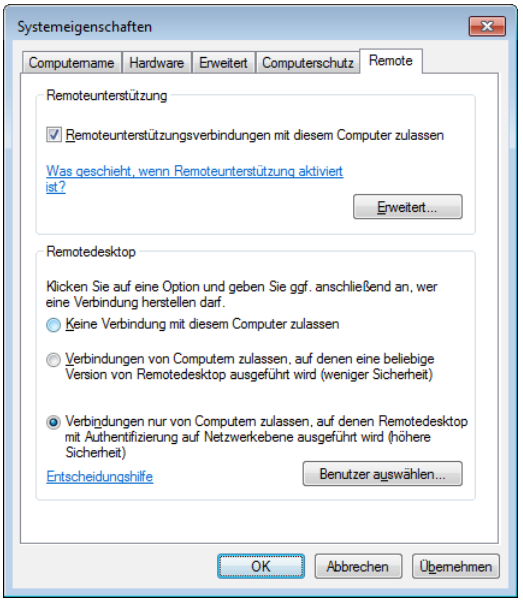

Systemeigenschaften
Computername
Hardware
Erweitert
Computerschutz
Remote
Remoteunterstützung
Remoteunterstützungsverbindungen mit diesem Computer zulassen
Was geschieht, wenn Remoteunterstützung aktiviert ist?
Erweitert...
Remotedesktop
Klicken Sie auf eine Option und geben Sie ggf. anschließend an, wer eine Verbindung herstellen darf.
Keine Verbindung mit diesem Computer zulassen
Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird (weniger Sicherheit)
Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird (höhere Sicherheit)
Entscheidungshilfe
Benutzer auswählen...
OK
Abbrechen
Übernehmen

Abbildung 7.26 Remotedesktopeigenschaften

9. Klicken Sie im Dialogfeld *Remotedesktopbenutzer* auf *Hinzufügen*. Geben Sie im Dialogfeld *Benutzer auswählen* den Namen **Cassie_Hicks** ein und klicken Sie dann auf *OK*. Schließen Sie die beiden Dialogfelder *Remotedesktopbenutzer* und *Systemeigenschaften* jeweils mit einem Klick auf *OK*.
10. Melden Sie sich von *Aberdeen* ab, aber lassen Sie den Computer eingeschaltet. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
11. Klicken Sie auf *Start* und geben Sie im Textfeld *Programme/Dateien durchsuchen* **Remotedesktopverbindung** ein. Klicken Sie auf den Eintrag *Remotedesktopverbindung*.
12. Klicken Sie im Dialogfeld *Remotedesktopverbindung* auf *Optionen*. Geben Sie im Textfeld *Computer* **Aberdeen** ein und im Textfeld *Benutzername* **Cassie_Hicks** (Abbildung 7.27). Klicken Sie auf *Verbinden*.
13. Geben Sie im Textfeld *Kennwort* des Dialogfelds *Windows-Sicherheit* das Kennwort **P@ssw0rd** für das Benutzerkonto *Cassie_Hicks* ein und klicken Sie auf *OK*.
14. Wenn Sie die Warnung erhalten, dass sich die Identität des Remotecomputers nicht überprüfen lässt (Abbildung 7.28), klicken Sie auf *Ja*.
15. Nachdem die Verbindung zustande gekommen ist, klicken Sie auf das *Start*-Menü und geben im Textfeld *Programme/Dateien durchsuchen* **PowerShell** ein. Klicken Sie auf den Eintrag *Windows PowerShell*.
16. Geben Sie in der *PowerShell*-Eingabeaufforderung den Befehl **$env:ComputerName; $env:UserName** ein und drücken Sie die EINGABETASTE. Überprüfen Sie, ob die Werte *Aberdeen* und *Cassie Hicks* angezeigt werden. Schließen Sie das *PowerShell*-Fenster und melden Sie sich vom Computer *Aberdeen* ab.

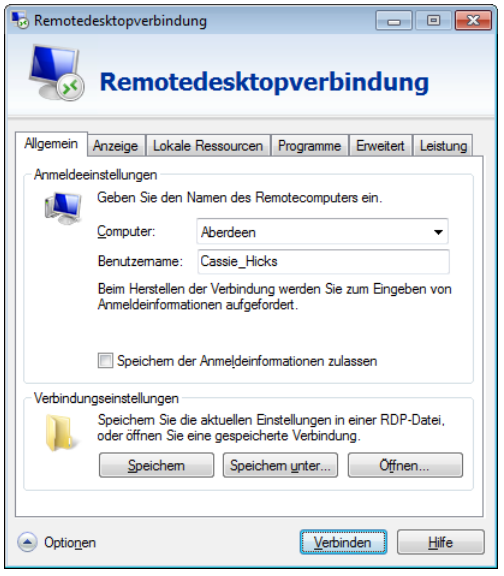


Abbildung 7.27 Der Remotedesktopclient

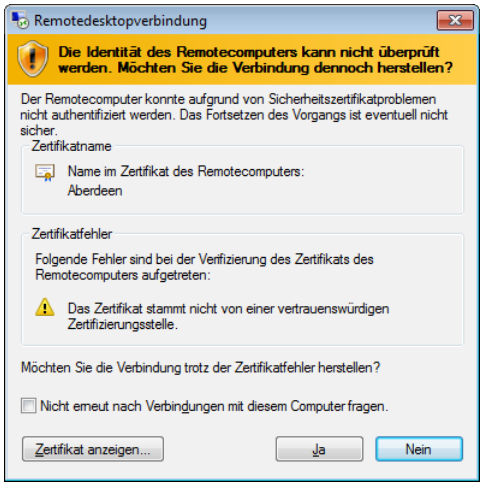

Remotedesktopverbindung
Die Identität des Remotecomputers kann nicht überprüft werden. Möchten Sie die Verbindung dennoch herstellen?
Der Remotecomputer konnte aufgrund von Sicherheitszertifikatproblemen nicht authentifiziert werden. Das Fortsetzen des Vorgangs ist eventuell nicht sicher.
Zertifikatname
Name im Zertifikat des Remotecomputers:
Aberdeen
Zertifikatfehler
Folgende Fehler sind bei der Verifizierung des Zertifikats des Remotecomputers aufgetreten:
Das Zertifikat stammt nicht von einer vertrauenswürdigen Zertifizierungsstelle.
Möchten Sie die Verbindung trotz der Zertifikatfehler herstellen?
Nicht erneut nach Verbindungen mit diesem Computer fragen.
Zertifikat anzeigen...
Ja
Nein

Abbildung 7.28 Überprüfen des Remotecomputers

Übung 2 Verwenden von Windows PowerShell und WinRS zur Remoteverwaltung

In dieser Übung richten Sie einen Windows 7-Clientcomputer so ein, dass er mit Windows PowerShell und WinRS remote verwaltet werden kann. Sie verwenden einige Befehle remote, um zu überprüfen, ob die Konfiguration richtig ist.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Aberdeen* an.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Geben Sie den Befehl **WinRM quickconfig** ein und drücken Sie die EINGABETASTE. Wenn Sie dazu aufgefordert werden, drücken Sie jeweils die Taste Y und anschließend die EINGABETASTE (Abbildung 7.29).

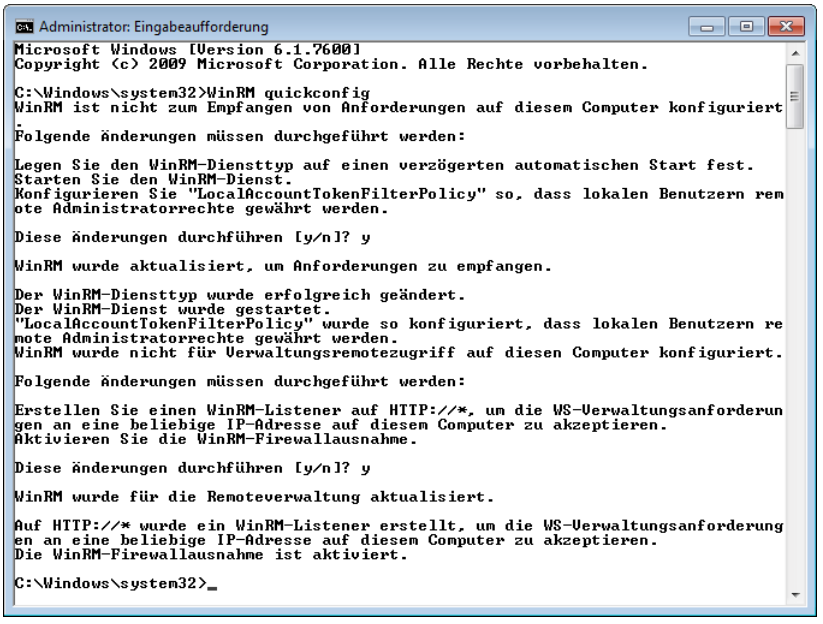

Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Windows\system32>WinRM quickconfig
WinRM ist nicht zum Empfangen von Anforderungen auf diesem Computer konfiguriert.
Folgende Änderungen müssen durchgeführt werden:
Legen Sie den WinRM-Diensttyp auf einen verzögerten automatischen Start fest.
Starten Sie den WinRM-Dienst.
Konfigurieren Sie "LocalAccountTokenFilterPolicy" so, dass lokalen Benutzern rem
ote Administratorrechte gewährt werden.
Diese Änderungen durchführen [y/n]? y
WinRM wurde aktualisiert, um Anforderungen zu empfangen.
Der WinRM-Diensttyp wurde erfolgreich geändert.
Der WinRM-Dienst wurde gestartet.
"LocalAccountTokenFilterPolicy" wurde so konfiguriert, dass lokalen Benutzern re
mote Administratorrechte gewährt werden.
WinRM wurde nicht für Verwaltungsremotezugriff auf diesen Computer konfiguriert.
Folgende Änderungen müssen durchgeführt werden:
Erstellen Sie einen WinRM-Listener auf HTTP://*, um die WS-Verwaltungsanforderun
gen an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Aktivieren Sie die WinRM-Firewallausnahme.
Diese Änderungen durchführen [y/n]? y
WinRM wurde für die Remoteverwaltung aktualisiert.
Auf HTTP://* wurde ein WinRM-Listener erstellt, um die WS-Verwaltungsanforderung
en an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Die WinRM-Firewallausnahme ist aktiviert.
C:\Windows\system32>

Abbildung 7.29 `WinRM quickconfig`

3. Schließen Sie das Fenster *Eingabeaufforderung* und melden Sie sich vom Computer *Aberdeen* ab, aber lassen Sie den Computer eingeschaltet.
4. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
5. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
6. Geben Sie den Befehl **WinRM quickconfig** ein und drücken Sie die EINGABETASTE. Wenn Sie dazu aufgefordert werden, drücken Sie die Taste Y und dann die EINGABETASTE.
7. Geben Sie den Befehl **winrm set winrm/config/client @{TrustedHosts="Aberdeen"}** ein und drücken Sie die EINGABETASTE.
8. Geben Sie den Befehl **whoami** ein**.** Überprüfen Sie, ob das Ergebnis *Canberra\Kim_Akers* lautet.
9. Geben Sie den Befehl **winrs -r:Aberdeen whoami** ein**.** Überprüfen Sie, ob das Ergebnis *Aberdeen\Kim_Akers* lautet.
10. Geben Sie den Befehl **ipconfig** ein**.** Merken Sie sich die IP-Adresse.
11. Geben Sie den Befehl **winrs -r:Aberdeen ipconfig** ein**.** Beachten Sie, dass nun eine andere IP-Adresse angezeigt wird.
12. Geben Sie den Befehl **PowerShell** ein und drücken Sie die EINGABETASTE. Windows PowerShell wird gestartet.
13. Geben Sie den Befehl **Get-Process | Sort-Object -Property CPU -Descending | Select -First 10** ein und drücken Sie die EINGABETASTE. Es wird eine Liste der ersten 10 Prozesse nach Prozessorauslastung auf *Canberra* angezeigt.

14. Geben Sie den Befehl **icm Aberdeen { Get-Process | Sort-Object -Property CPU -Descending | Select -First 10 }** ein und drücken Sie die EINGABETASTE. Dadurch wird eine Liste der ersten 10 Prozesse nach Prozessorauslastung auf *Aberdeen* angezeigt.
15. Schließen Sie Windows PowerShell und die Eingabeaufforderung.

Zusammenfassung der Lektion

- Remotedesktop ermöglicht es, eine Verbindung mit einem Remotecomputer herzustellen und dessen Desktop so zu sehen, als wäre man direkt angemeldet.
- Wenn Remotedesktop mit einer Authentifizierung auf Netzwerkebene aktiviert ist, können nur Clients eine Verbindung herstellen, auf denen Windows Vista oder Windows 7 ausgeführt wird. Auch Windows XP-Clients mit SP3 können eine Verbindung herstellen, allerdings wird dies nicht standardmäßig unterstützt und erfordert eine spezielle Konfiguration.
- Standardbenutzer müssen Mitglieder der Gruppe *Remotedesktopbenutzer* werden, bevor sie mit Remotedesktop eine Verbindung mit einem Windows 7-Client herstellen können.
- Auf einem Client, den Sie mit WinRS oder Windows PowerShell remote verwalten möchten, müssen Sie in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `WinRM quickconfig` verwenden. `WinRM quickconfig` konfiguriert den Windows-Remoteverwaltungsdienst und passende Firewallregeln und aktiviert den WinRM-Listener.
- Um einen Befehl auf einem Remotehost namens *Hostname* zur Ausführung zu bringen, können Sie den Befehl `winrs -r:Hostname` verwenden.
- Nur Windows PowerShell V2 und höher eignet sich zur Remoteverwaltung von Windows 7. Windows PowerShell V2 ist die Standardversion von Windows PowerShell, die in Windows 7 enthalten ist.
- Sie können den Befehl `icm Hostname` verwenden, um PowerShell-Befehle auf dem Remotecomputer *Hostname* auszuführen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 2, »Windows 7-Remoteverwaltung«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie müssen mit einem Computer, auf dem Windows XP mit SP2 installiert ist, einen Windows 7-Computer verwalten, wenn auf dem Windows 7-Computer kein Benutzer angemeldet ist. Sie möchten, dass die Verbindungen so sicher wie möglich sind. Welche der folgenden Einstellungen sollten Sie auf der Registerkarte *Remote* des Dialogfelds *Systemeigenschaften* vornehmen?

A. *Remoteunterstützung*: *Remoteunterstützungsverbindungen mit diesem Computer zulassen*
B. *Remotedesktop*: *Keine Verbindung mit diesem Computer zulassen*
C. *Remotedesktop*: *Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird*
D. *Remotedesktop*: *Verbindungen nur von Computern zulassen, die Remotedesktop mit Authentifizierung auf Netzwerkebene verwenden*

2. Sie möchten auf einem Windows 7-Computer namens *Alpha* einen Windows 7-Client namens *Beta* mit Windows PowerShell verwalten. Welcher der folgenden Arbeitsschritte ist dafür erforderlich?
   A. Sie verwenden auf dem Computer *Alpha* in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `WinRM quickconfig`.
   B. Sie verwenden auf dem Computer *Beta* in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `WinRM quickconfig`.
   C. Sie erstellen auf dem Computer *Alpha* eine WFAS-Regel für TCP-Port 80.
   D. Sie erstellen auf dem Computer *Beta* eine WFAS-Regel für TCP-Port 80.
3. Sie sind auf einem Windows 7-Computer namens *Canberra* angemeldet. Sie möchten die MAC-Adresse (Media Access Control) des Windows 7-Computers *Aberdeen* ermitteln, der zu einem anderen Subnetz gehört. Beide Computer sind Mitglieder derselben Domäne. Ihr Domänenbenutzerkonto ist auf beiden Computern Mitglied der lokalen Gruppe *Administratoren*. Auf allen Windows 7-Clients Ihrer Organisation wurde der Befehl `WinRM quickconfig` ausgeführt. Mit welchem der folgenden Befehle erhalten Sie die gewünschte Information?
   A. `nslookup` *`Aberdeen`*
   B. `winrs -r:`*`Aberdeen`* `ipconfig /all`
   C. `winrs -r:`*`Canberra`* `ipconfig /all`
   D. `arp -a`
4. Mit welchem der folgenden Windows PowerShell-Befehle können Sie auf einem Windows 7-Computer namens *Canberra* eine Liste der Prozesse einschließlich Prozessor- und Speicherverwendung vom Windows 7-Client *Aberdeen* abrufen?
   A. `icm Canberra {Get-Process}`
   B. `icm Aberdeen {Get-Process}`
   C. `winrs -r:`*`Aberdeen`* `Get-Process`
   D. `winrs -r:`*`Canberra`* `Get-Process`
5. Welcher der folgenden Gründe könnte erklären, warum ein Helfer keine Remoteunterstützungsverbindung mit einem anderen Computer erhält, obwohl die beiden eigenständigen Windows 7-Computer beide zum selben Subnetz gehören?
   A. Der WinRM-Dienst ist auf *Aberdeen* deaktiviert.
   B. Der Client *Aberdeen* wurde so konfiguriert, dass er Remotedesktopsitzungen nur mit Authentifizierung auf Netzwerkebene durchführt.
   C. Der Helfer ist auf *Aberdeen* kein Mitglied der lokalen Gruppe *Remotedesktopbenutzer*.
   D. Das Remoteunterstützungsprogramm wurde auf dem Client *Aberdeen* beendet.

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Die Windows-Firewall kann nur für Anwendungen und Funktionen konfiguriert werden.
- WFAS kann für Anwendungen, Funktionen, Dienste und Ports konfiguriert werden. Es ist möglich, für WFAS-Regeln Authentifizierungs- und Bereichsoptionen zu konfigurieren.
- Die Remoteunterstützung ermöglicht es einem Benutzer, eine Unterstützungsanforderung an einen Helfer zu schicken, die es dem Helfer ermöglicht, den Desktop des Benutzers zu sehen. Es gibt verschiedene Sicherheitsvorkehrungen, die den Helfer daran hindern, den Computer des Benutzers gegen den Willen des Benutzers zu übernehmen.
- Remotedesktop ermöglicht es einem Benutzer, eine neue Sitzung einzuleiten oder eine Verbindung zu einer vorhandenen Sitzung zu erstellen, die der Benutzer auf einem Windows 7-Remoteclient erstellt hat.
- Der Windows-Remoteverwaltungsdienst ermöglicht es, Befehlszeilenprogramme und Windows PowerShell-Skripts für Windows 7-Clients remote auszuführen.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Verbindungssicherheitsregel**
- **Eingehende Regel**
- **Ausgehende Regel**
- **Windows-Remoteshell**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie Ihr Wissen zum Stoff dieses Kapitels an. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: Client-Firewalls an einer Universität

Sie sind an der örtlichen Universität für Desktops zuständig. Auf allen Clientcomputern der Universität wurde Windows 7 Enterprise installiert. Ihnen liegen mehrere Supportanforderungen vor. Die erste Anforderung stammt von einem Akademiker, der auf seinem Laptop eine Website betreiben möchte, wenn er auf Konferenzen Präsentationen vorführt und mit einem Ad-hoc-Netzwerk verbunden ist. Die Besucher seiner Präsentationen sollen eine Verbindung mit der Website herstellen können, um Informationen herunterzuladen, aber andere Leute sollen keine Verbindung herstellen können. Die zweite Anforderung stammt von Studenten, die auf USB-Flashlaufwerken eine Anwendung für den Dateiaustausch betreiben. Sie wissen, welchen Port die Anwendung benutzt, aber der Name der Anwendung scheint zu variieren. Die dritte Anforderung stammt von Teilnehmern eines Aufbaustudiums, in deren Kurs 25 eigenständige Windows 7-Computer verwendet werden. Sie möchten sicherstellen, dass alle Computer über dieselbe WFAS-Konfiguration verfügen.

Beantworten Sie nun folgende Fragen:

1. Was tun Sie bei der ersten Supportanforderung?
2. Was tun Sie bei der zweiten Supportanforderung?
3. Was tun Sie bei der dritten Supportanforderung?

Übung 2: Desktopunterstützung in der Antarktis

Ihre Organisation ist für den Support einer kleinen Forschungsstation in der Antarktis zuständig. Die Person, die normalerweise vor Ort den IT-Support übernimmt, ist krank geworden und wird die nächste Woche auf der Krankenstation verbringen. Nun ist es Ihre Aufgabe, für die Clientcomputer der 30 Wissenschaftler Support zu leisten, die in der Forschungsstation leben und arbeiten. Ihr Büro in Tasmanien ist über eine Hochgeschwindigkeits-Internetverbindung mit der Forschungsstation verbunden. Auf allen Windows 7-Clients wurde Remotedesktop aktiviert.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Eine der Wissenschaftlerinnen braucht auf Ihrem Windows 7-Clientcomputer eine Anwendung, die Sie nicht über Gruppenrichtlinien bereitstellen können. Sie haben zwar die Möglichkeit, Ihre Berechtigungen auf dem Computer anzuheben, aber die Wissenschaftlerin kann dies nicht. Wie lösen Sie das Problem?
2. Ein anderer Mitarbeiter aus dem Büro in Tasmanien muss eine Verbindung mit einem Windows 7-Client aus der Forschungsstation herstellen, um einige wissenschaftliche Ergebnisse zu überprüfen, aber es gelingt ihm nicht. Sie überprüfen die Sache und stellen fest, dass Sie eine Remotedesktopverbindung einrichten können. Wie lösen Sie das Problem?
3. Sie müssen die Windows 7-Clients mit Windows PowerShell-Skripts remote verwalten. Welche Vorbereitungen treffen Sie?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Die Windows-Firewall konfigurieren

- **Übung 1** Konfigurieren Sie eine eingehende WFAS-Regel für den UDP-Port 1138 für die IP-Adressen von 10.10.10.1 und 10.10.10.255.
- **Übung 2** Konfigurieren Sie eine eingehende WFAS-Regel für das Programm *Calc.exe* aus dem Ordner C:*Windows**System32*.

Konfigurieren der Remoteverwaltung

- **Übung 1** Stellen Sie einen WinRS-Befehl zusammen, der eine Liste aller lokalen Gruppen liefert, die es auf einem Windows 7-Remoteclient gibt, und wenden Sie den Befehl an.
- **Übung 2** Erstellen Sie ein Windows PowerShell-Skript, das den freien Speicherplatz auf den Volumes eines Remotecomputers angibt.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

KAPITEL 8

BranchCache und Ressourcenfreigabe

In der Arbeitswelt werden nur selten Dokumente erstellt, die nicht von anderen gelesen werden sollen. Der Aufwand für die Erstellung von Dokumenten ist gewöhnlich nur sinnvoll, wenn auch andere Mitarbeiter der Organisation die Dokumente erhalten. Häufig verbringen die Leute zahllose Stunden mit der Erstellung und Formatierung von Dokumenten in Microsoft Office Word, weil sie erwarten, dass andere diese Dokumente lesen. Sie schreiben Dokumente, um *anderen* Leuten Ideen zu erläutern oder sie mit Informationen zu versorgen, denn gewöhnlich ist es nicht nötig, sich selbst etwas schriftlich zu erklären. Der erste Teil dieses Kapitels beschreibt die Methoden, mit denen Sie auf Windows 7-Computern Daten freigeben. Dazu zählen zum Beispiel die einfache Dateifreigabe in Heimnetzgruppen oder die etwas kompliziertere Methode der Konfiguration von freigegebenen Ordnern. Im zweiten Teil des Kapitels wird die Beschränkung der Dateifreigabe besprochen, mit der Sie dafür sorgen können, dass die Daten nur für die vorgesehenen Leute einsehbar sind. Das erreichen Sie durch eine entsprechende Vergabe von Berechtigungen für Dateien und Ordner und durch eine Verschlüsselung der Daten, wobei nur bestimmte Leute die Daten wieder entschlüsseln können. Im letzten Teil dieses Kapitels geht es um die Beschleunigung des Datenzugriffs in kleinen Zweigstellen von größeren Organisationen. Dabei wird ein neues Windows 7-Feature namens BranchCache verwendet.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von freigegebenen Ressourcen
- Konfigurieren des Datei- und Ordnerzugangs
- Konfigurieren von BranchCache

Lektionen in diesem Kapitel:

- Lektion 1: Freigeben von Ressourcen 421
- Lektion 2: Ordner- und Dateizugriff 440
- Lektion 3: Verwalten von BranchCache 459

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels ist folgende Vorbereitung erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Client-PC namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.

Praxistipp

Orin Thomas

Die Freigabe von Dateien und Ordnern auf Clients statt auf Servern kann zwar in kleinen Firmen sinnvoll sein, die keinen speziellen Dateiserver bereitstellen möchten, aber wenn man dabei nicht sorgfältig vorgeht, können sich daraus erfahrungsgemäß viele Probleme ergeben. Wahrscheinlich liegt es daran, dass die Leute über freigegebene Ordner auf einem Server ganz anders denken als über freigegebene Ordner auf Clients. Wenn ein Dateiserver verwendet wird, wissen die Leute meistens sehr genau, dass Dateien, die an diesem Ort gespeichert werden, für andere Leute aus der Organisation sichtbar sind. Bei der Bereitstellung von Dateiservern ist es sehr einfach, Dateifreigaben auf der Basis von Gruppenmitgliedschaften einzurichten, und die Leute erinnern sich daran, dass eine Datei, die nur für Manager verfügbar sein soll, in den freigegebenen Ordner *Manager* gehört. Auf Clientcomputern lässt sich das zwar auch erreichen, aber es ist aufwendiger, auf jedem Clientcomputer verschiedene Freigaben mit bestimmten Berechtigungen einzurichten. Noch aufwendiger ist es, die Leute, die an diesen Computern arbeiten, dazu zu bringen, sich das Vorgehen zur Einrichtung von Berechtigungen zu merken.

Einer meiner Kollegen hatte mit einem Fall zu tun, bei dem ein Manager einer Firma, die zu seinen Klienten zählte, Leistungsbeurteilungen in einem lokalen Ordner speicherte, der für alle anderen Benutzer im Netzwerk sichtbar war. Es war zwar ein spezieller freigegebener Ordner verfügbar, dessen Dokumente nur für den Direktor der Firma und seinen Assistenten zugänglich waren, aber der Manager hatte einfach nicht zugehört, als ihm dies erklärt wurde. Er ging von der Annahme aus, dass niemand die Beurteilungen zu sehen bekäme, weil er nur seinem Assistenten und dem Firmendirektor erzählt hatte, dass die Dokumente im freigegebenen Ordner liegen.

Freigegebene Drucker können zu ähnlichen Problemen führen. In vielen kleinen Firmen erhalten die Leute um so bessere Hardware, je höher sie in der Hierarchie stehen. Die Person, die den leistungsfähigsten Drucker erhält, erhält ihn deswegen, weil ihr die Firma gehört und sie die Kaufaufträge unterschreibt. Irgendwann wird der Drucker freigegeben, damit die Leute, die beispielsweise doppelseitig drucken müssen, dies auch tun können. Der Nachteil ist, dass diese Leute dann zum Büro des Betreffenden gehen müssen, um die Ausdrucke abzuholen. Ich kenne eine Organisation, in der mehrere Leute Schlüssel für das Büro des Chefs hatten, damit sie ihre Ausdrucke auch dann abholen konnten, wenn er unterwegs war. Statt den Drucker einfach an einen leichter zugänglichen Ort zu stellen, hat der Chef schließlich den Kauf eines weiteren Druckers genehmigt.

Lektion 1: Freigeben von Ressourcen

In den meisten Heimnetzwerken und kleinen Geschäften ist es nicht erforderlich, einen speziellen Datei- und Druckserver einzurichten. Gewöhnlich gibt es nur ein paar Computer, und die Zahl der Dateien, die unter den Mitarbeitern ausgetauscht werden müssen, ist nicht groß. Wenn Sie nicht über einen Datei- und Druckserver verfügen, können Sie die Freigabeoptionen von Windows 7 verwenden, um Dateien, Ordner und Drucker gemeinsam zu verwenden. Windows 7 bietet ein neues Feature namens Heimnetzgruppen, mit denen sich die Freigabe von Dateien und Druckern in kleinen Netzwerken vereinfachen lässt, in denen es keine Active Directory-Domänendienste gibt.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren der Einstellungen von Heimnetzgruppen
- Konfigurieren der Freigabeeinstellungen im Netzwerk- und Freigabecenter
- Freigeben von Ordnern
- Verwalten von Druckerberechtigungen

Veranschlagte Zeit für diese Lektion: 40 Minuten

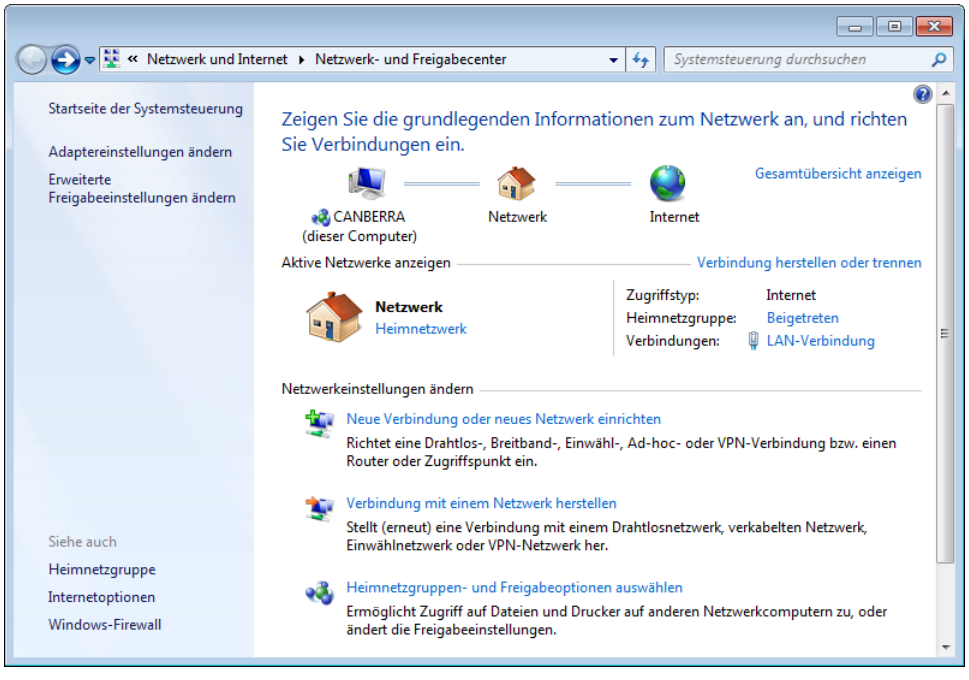

« Netzwerk und Internet ▸ Netzwerk- und Freigabecenter
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Adaptereinstellungen ändern
Erweiterte Freigabeeinstellungen ändern
Zeigen Sie die grundlegenden Informationen zum Netzwerk an, und richten Sie Verbindungen ein.
Gesamtübersicht anzeigen
CANBERRA (dieser Computer)
Netzwerk
Internet
Aktive Netzwerke anzeigen
Verbindung herstellen oder trennen
Netzwerk
Heimnetzwerk
Zugriffstyp: Internet
Heimnetzgruppe: Beigetreten
Verbindungen: LAN-Verbindung
Netzwerkeinstellungen ändern
Neue Verbindung oder neues Netzwerk einrichten
Richtet eine Drahtlos-, Breitband-, Einwähl-, Ad-hoc- oder VPN-Verbindung bzw. einen Router oder Zugriffspunkt ein.
Verbindung mit einem Netzwerk herstellen
Stellt (erneut) eine Verbindung mit einem Drahtlosnetzwerk, verkabelten Netzwerk, Einwählnetzwerk oder VPN-Netzwerk her.
Heimnetzgruppen- und Freigabeoptionen auswählen
Ermöglicht Zugriff auf Dateien und Drucker auf anderen Netzwerkcomputern zu, oder ändert die Freigabeeinstellungen.
Siehe auch
Heimnetzgruppe
Internetoptionen
Windows-Firewall

Abbildung 8.1 Netzwerk- und Freigabecenter

Netzwerk- und Freigabecenter

Sie können das Netzwerk- und Freigabecenter (Abbildung 8.1) verwenden, um Heimnetzgruppen und erweiterte Freigabeoptionen zu konfigurieren. Im Netzwerk- und Freigabecenter können Sie auch überprüfen, mit welchen Netzwerken der Computer verbunden ist

und wie diese Netzwerke eingestuft werden. Mit diesem Tool können Sie die Einstufung der Netzwerke auch ändern. Aus einem Arbeitsplatznetzwerk können Sie zum Beispiel ein Heimnetzwerk machen, indem Sie unter dem Netzwerknamen auf *Arbeitsplatznetzwerk* klicken und dann im Dialogfeld *Netzwerkadresse festlegen* auf *Heimnetzwerk* klicken. Über die Freigabeoptionen der Heimnetzgruppe erfahren Sie mehr im Verlauf dieser Lektion.

Um das Dialogfeld *Erweiterte Freigabeeinstellungen* zu öffnen, klicken Sie im Netzwerk- und Freigabecenter auf *Erweiterte Freigabeeinstellungen ändern*. In diesem Dialogfeld (Abbildung 8.2) können Sie die Freigabeoptionen für die verschiedenen Netzwerkprofile festlegen. Netzwerkprofile gelten auf Schnittstellenbasis. Wenn ein Windows 7-Computer über mehrere Netzwerkschnittstellen verfügt und zum Beispiel über eine Drahtlosnetzwerkkarte mit einem Heimnetzwerk verbunden ist und über DirectAccess auf ein Organisationsnetzwerk zugreift, kann für jede Schnittstelle ein anderes Netzwerkprofil gelten.

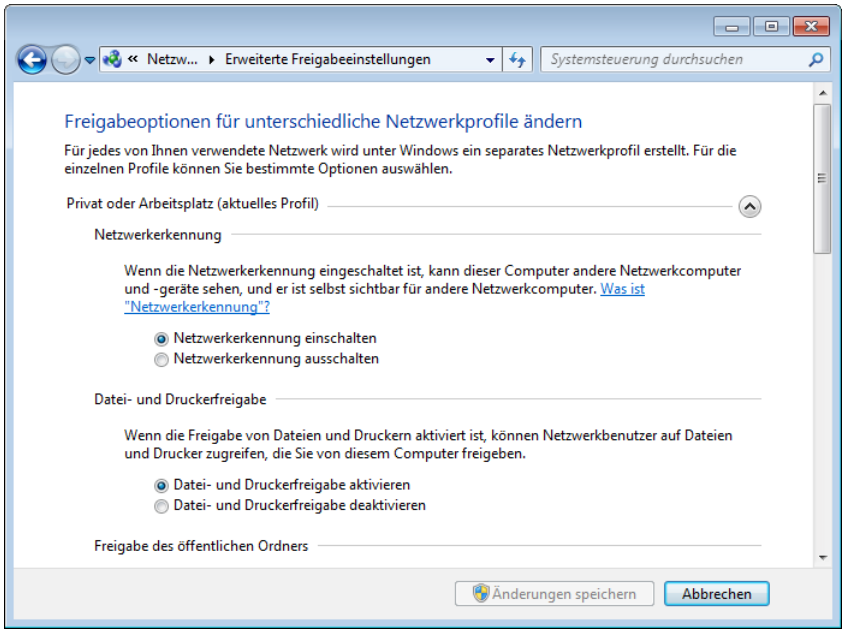

« Netzw... ▸ Erweiterte Freigabeeinstellungen
Systemsteuerung durchsuchen
Freigabeoptionen für unterschiedliche Netzwerkprofile ändern
Für jedes von Ihnen verwendete Netzwerk wird unter Windows ein separates Netzwerkprofil erstellt. Für die einzelnen Profile können Sie bestimmte Optionen auswählen.
Privat oder Arbeitsplatz (aktuelles Profil)
Netzwerkerkennung
Wenn die Netzwerkerkennung eingeschaltet ist, kann dieser Computer andere Netzwerkcomputer und -geräte sehen, und er ist selbst sichtbar für andere Netzwerkcomputer. Was ist "Netzwerkerkennung"?
Netzwerkerkennung einschalten
Netzwerkerkennung ausschalten
Datei- und Druckerfreigabe
Wenn die Freigabe von Dateien und Druckern aktiviert ist, können Netzwerkbenutzer auf Dateien und Drucker zugreifen, die Sie von diesem Computer freigeben.
Datei- und Druckerfreigabe aktivieren
Datei- und Druckerfreigabe deaktivieren
Freigabe des öffentlichen Ordners
Änderungen speichern
Abbrechen

Abbildung 8.2 Erweiterte Freigabeeinstellungen

In den erweiterten Freigabeeinstellungen können Sie folgende Optionen aktivieren, deaktivieren oder konfigurieren:

- **Netzwerkerkennung** Die Netzwerkerkennung ermöglicht es einem Windows 7-Computer, andere Computer und Geräte im Netzwerk zu erkennen. Außerdem wird der Computer für andere Computer im Netzwerk sichtbar. Eine Deaktivierung der Netzwerkerkennung schaltet andere Arten der Freigabe nicht ab.
- **Datei- und Druckerfreigabe** Diese Einstellung ermöglicht die gemeinsame Nutzung von Dateien und Druckern im Netzwerk.
- **Freigabe des öffentlichen Ordners** Eine Aktivierung dieser Einstellung ermöglicht es anderen Benutzern im Netzwerk, in einen öffentlichen Ordner zu schreiben oder aus ihm zu lesen. Wenn Sie diese Einstellung deaktivieren, erhalten andere Benutzer nur

Schreib- und Lesezugriff auf die freigegebenen Ordner, in denen sie über die entsprechenden Berechtigungen verfügen.

- **Medienstreaming** Wenn Sie diese Einstellung aktivieren, können andere Benutzer im Netzwerk auf Bilder, Musik und Videos zugreifen, die auf dem Windows 7-Computer gespeichert sind. Außerdem kann der Windows 7-Computer Bilder, Musik und Videos auf anderen Windows 7-Computern im Netzwerk lokalisieren.
- **Dateifreigabeverbindungen** Diese Option ermöglicht die Wahl zwischen dem Schutz der Dateifreigabeverbindungen mit einer 128-Bit-Verschlüsselung oder mit einer 40- oder 56-Bit-Verschlüsselung. Wählen Sie die 40- oder 56-Bit-Verschlüsselung für Geräte, die die 128-Bit-Verschlüsselung nicht unterstützen.
- **Kennwortgeschütztes Freigeben** Die Aktivierung dieser Option bedeutet, dass nur Benutzer, die auf dem Computer über lokale Konten verfügen, auf freigegebene Ressourcen zugreifen können. Damit auch Benutzer auf freigegebene Ressourcen zugreifen können, die nicht über lokale Konten verfügen, müssen Sie diese Option deaktivieren.
- **Heimnetzgruppen-Verbindungen** Diese Option entscheidet darüber, wie die Authentifizierung für Verbindungen mit Ressourcen der Heimnetzgruppe funktioniert. Wenn auf allen Computern der Heimnetzgruppe dieselben Benutzernamen und Kennwörter eingerichtet wurden, können Sie diese Option aktivieren, damit Windows die Verbindungen der Heimnetzgruppe verwaltet. Gibt es unterschiedliche Benutzerkonten und Kennwörter, sollten Sie diese Option so konfigurieren, dass Benutzerkonten und Kennwörter für Verbindungen zu anderen Computern verwendet werden. Diese Option ist nur im Profil *Privat oder Arbeitsplatz* verfügbar.

Heimnetzgruppen

Heimnetzgruppen sind eine einfache Methode, die gemeinsame Verwendung von Ressourcen in einem Heimnetzwerk zu ermöglichen. Sie können Heimnetzgruppen nur in Netzwerken verwenden, die Sie als Heimnetzwerke eingerichtet haben. In einem Domänennetzwerk können Sie keine Heimnetzgruppe einrichten, aber Sie können einer vorhandenen Heimnetzgruppe beitreten (Abbildung 8.3). Beispielsweise können Sie einer vorhandenen Heimnetzgruppe beitreten, wenn Sie Ihren Windows 7-Computer in Ihrem Heimnetzwerk verwenden, aber gleichzeitig über DirectAccess eine Verbindung mit dem Domänennetzwerk Ihrer Organisation hergestellt haben.

Heimnetzgruppen werden im Windows-Explorer unter einem separaten Knoten dargestellt. Windows 7 zeigt Heimnetzgruppen mit Benutzer- und Computernamen an, weil jeder Benutzer auf einem Windows 7-Computer andere Ressourcen für das Netzwerk freigibt, je nach seinen individuellen Freigabeeinstellungen. Abbildung 8.4 zeigt die Heimnetzgruppen *Don_Hall (CANBERRA)* und *Kim_Akers (CANBERRA)*. Zur Heimnetzgruppe *Kim_Akers (CANBERRA)* gehört eine benutzerdefinierte Bibliothek namens *Wissenschaftliche_Daten*. Diese Bibliothek erstellen Sie in einer Übung am Ende der Lektion.

Zwar können nur Benutzer mit Administratorrechten die Heimnetzgruppe aktivieren, aber jeder Standardbenutzer kann die Bibliotheken auswählen, die er in der Heimnetzgruppe freigeben möchte. *Kim_Akers* könnte beispielsweise ihre Bibliotheken *Dokumente*, *Musik*, *Bilder* und *Videos* freigeben, während *Don_Hall* vielleicht nur seine Bibliothek *Dokumente* freigibt. Benutzer brauchen nicht angemeldet zu sein, damit ihre Heimnetzgruppen für andere Benutzer im Netzwerk verfügbar sind. Die Heimnetzgruppenfreigabe jedes Benutzers ist verfügbar,

solange der Computer, auf dem sie liegt, eingeschaltet ist, mit dem Heimnetzwerk verbunden ist und einwandfrei funktioniert.

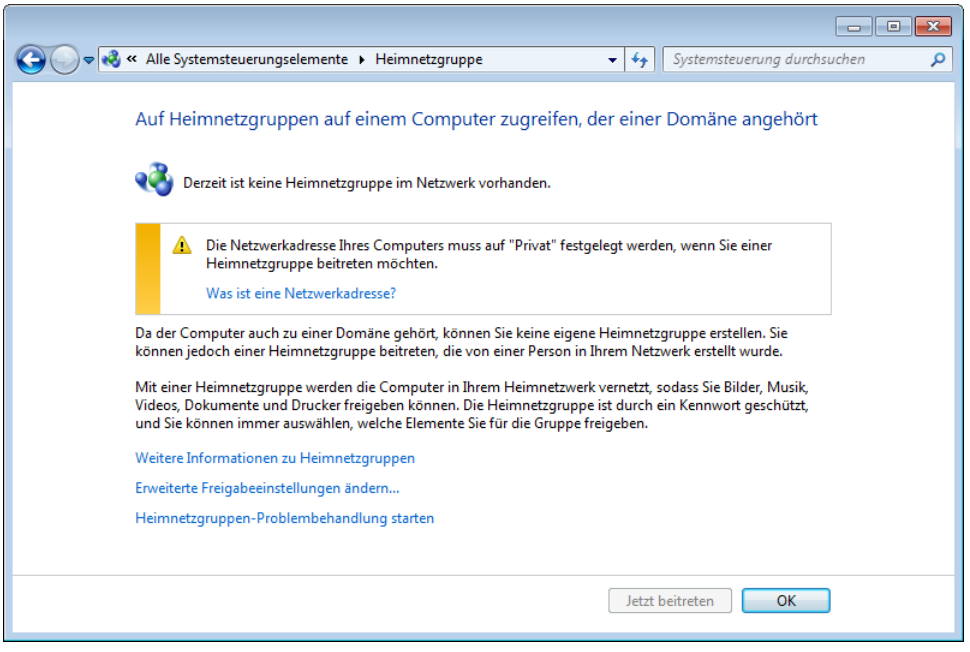

« Alle Systemsteuerungselemente ▸ Heimnetzgruppe
Systemsteuerung durchsuchen
Auf Heimnetzgruppen auf einem Computer zugreifen, der einer Domäne angehört
Derzeit ist keine Heimnetzgruppe im Netzwerk vorhanden.
Die Netzwerkadresse Ihres Computers muss auf "Privat" festgelegt werden, wenn Sie einer Heimnetzgruppe beitreten möchten.
Was ist eine Netzwerkadresse?
Da der Computer auch zu einer Domäne gehört, können Sie keine eigene Heimnetzgruppe erstellen. Sie können jedoch einer Heimnetzgruppe beitreten, die von einer Person in Ihrem Netzwerk erstellt wurde.
Mit einer Heimnetzgruppe werden die Computer in Ihrem Heimnetzwerk vernetzt, sodass Sie Bilder, Musik, Videos, Dokumente und Drucker freigeben können. Die Heimnetzgruppe ist durch ein Kennwort geschützt, und Sie können immer auswählen, welche Elemente Sie für die Gruppe freigeben.
Weitere Informationen zu Heimnetzgruppen
Erweiterte Freigabeeinstellungen ändern...
Heimnetzgruppen-Problembehandlung starten
Jetzt beitreten
OK

Abbildung 8.3 Es ist keine Heimnetzgruppe im Domänennetzwerk vorhanden

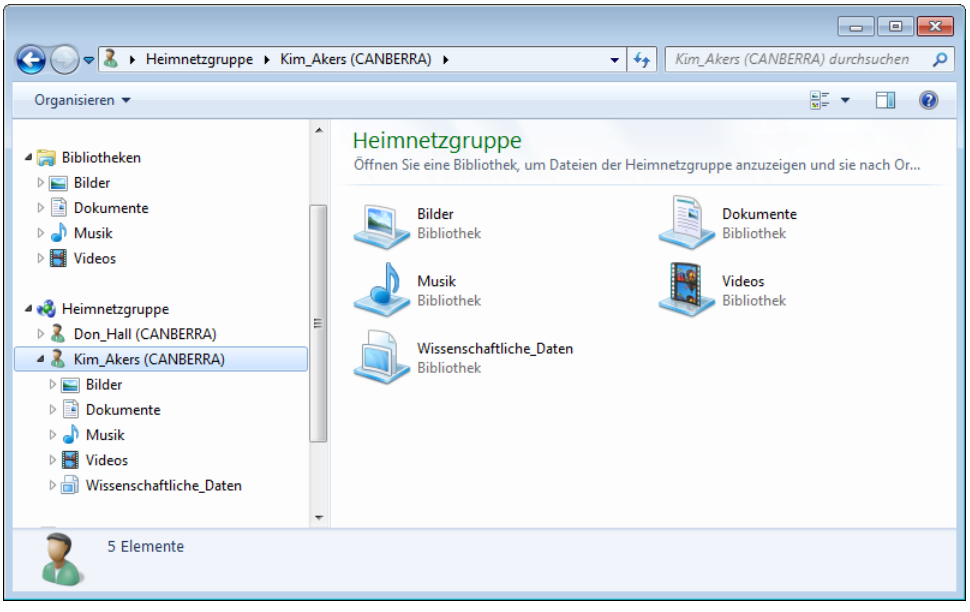


Abbildung 8.4 Anzeigen der Heimnetzgruppen

Wenn eine Heimnetzgruppe verfügbar ist, wird sie auf der Seite *Heimnetzgruppe* der Systemsteuerung angezeigt. Klicken Sie im Netzwerk- und Freigabecenter auf *Heimnetzgruppe*, um diese Seite zu öffnen.

So treten Sie einer Heimnetzgruppe bei, die im Netzwerk verfügbar ist:

1. Klicken Sie im Netzwerk- und Freigabecenter auf *Heimnetzgruppe*.
2. Wenn auf einem anderen Computer eine Heimnetzgruppe erkannt wird, wird sie auf dieser Seite angezeigt. Informieren Sie sich beim Ersteller der Heimnetzgruppe über das zu verwendende Kennwort und klicken Sie auf *Jetzt beitreten*.
3. Wählen Sie auf der Seite *Einer Heimnetzgruppe beitreten* die Objekte aus, die Sie für andere Benutzer des Heimnetzwerks freigeben möchten, und klicken Sie auf *Weiter*.

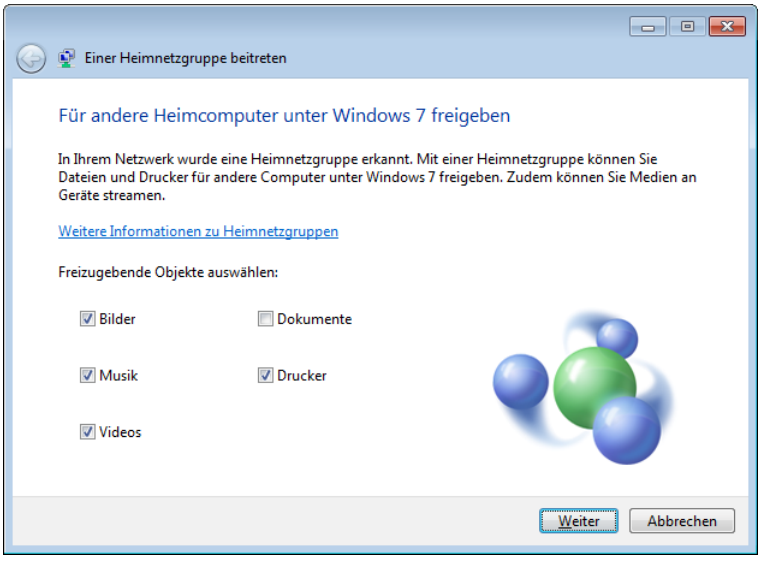

Einer Heimnetzgruppe beitreten
Für andere Heimcomputer unter Windows 7 freigeben
In Ihrem Netzwerk wurde eine Heimnetzgruppe erkannt. Mit einer Heimnetzgruppe können Sie Dateien und Drucker für andere Computer unter Windows 7 freigeben. Zudem können Sie Medien an Geräte streamen.
Weitere Informationen zu Heimnetzgruppen
Freizugebende Objekte auswählen:
Bilder
Dokumente
Musik
Drucker
Videos
Weiter
Abbrechen

Abbildung 8.5 Freigeben von Objekten in der Heimnetzgruppe

4. Geben Sie das Heimnetzgruppenkennwort ein, das Sie vom Ersteller der Heimnetzgruppe erhalten haben. Wenn das Kennwort akzeptiert wird, sind Sie der Heimnetzgruppe beigetreten.

Wenn Sie die Heimnetzgruppe verlassen möchten, klicken Sie im Netzwerk- und Freigabecenter auf *Heimnetzgruppe* und dann auf *Heimnetzgruppe verlassen*.

Freigegebene Ordner

Freigegebene Ordner ermöglichen anderen Benutzern im Netzwerk den Zugriff auf Daten, die auf Ihrem Computer in diesen Ordnern gespeichert sind. Einzelne Ordner können Sie freigeben, indem Sie sie mit der rechten Maustaste anklicken, *Eigenschaften* wählen und dann im Eigenschaftendialogfeld des Ordners auf die Registerkarte *Freigabe* klicken (Abbildung 8.6). Auf dieser Registerkarte werden zwei verschiedene Freigabeoptionen angeboten, *Freigabe* und *Erweiterte Freigabe*. Freigegebene Ordner können Sie auch verwenden, wenn Sie keine Heimnetzgruppen verwenden können, beispielsweise zur Freigabe von Ressourcen in einem Arbeitsplatznetzwerk.

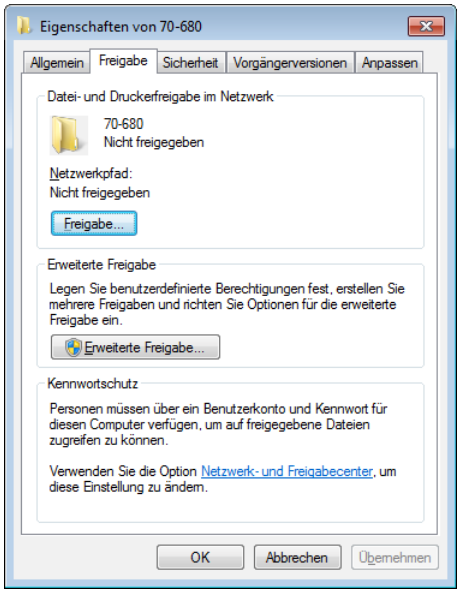


Abbildung 8.6 Die Registerkarte *Freigabe* aus dem Eigenschaftendialogfeld eines Ordners

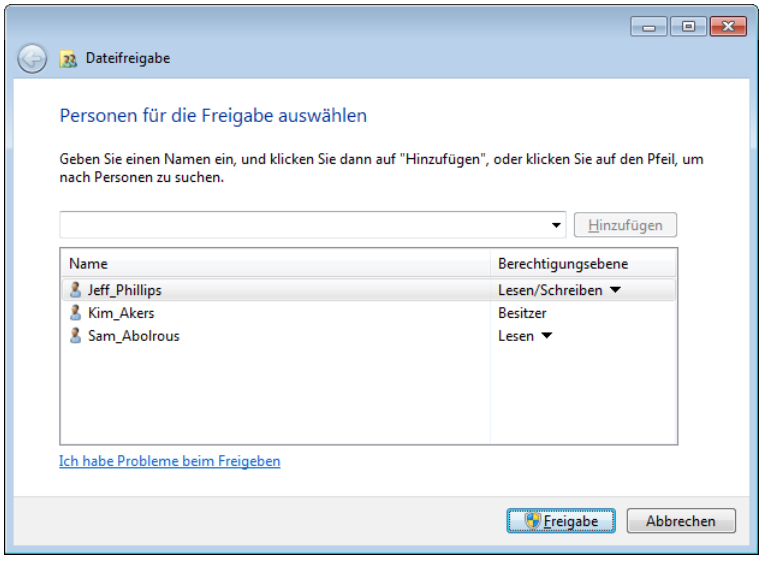


Abbildung 8.7 Einfache Dateifreigabe

Ein Klick auf *Freigabe* öffnet das Dialogfeld *Dateifreigabe* (Abbildung 8.7). In diesem Dialogfeld können Sie Freigabeberechtigungen für lokale Benutzerkonten, die Gruppe *Jeder* oder die *Heimnetzgruppe* festlegen. Wenn Sie einen Windows 7-Computer zu einer Domäne hinzufügen, können Sie Domänenbenutzerkonten und Domänengruppen angeben, aber keine lokalen Gruppen mehr. Das Benutzerkonto, mit dem Sie den Ordner freigeben, erhält automatisch die Berechtigung *Besitzer*. Es ist auch möglich, Konten die Berechtigung *Lesen*/

Schreiben zuzuweisen, mit der sie im freigegebenen Ordner Dateien hinzufügen, löschen und ändern können, oder die Berechtigung *Lesen*, mit der Benutzer auf Dateien aus dem freigegebenen Ordner zugreifen, sie aber nicht ändern oder löschen können.

Ein Klick auf *Erweiterte Freigabe* öffnet das gleichnamige Dialogfeld (Abbildung 8.8). In diesem Dialogfeld können Sie die Zahl der Benutzer beschränken, die Zugriff auf die Freigabe erhalten. Schränken Sie die Zahl ein, wenn es aus Leistungsgründen erforderlich ist. Nach einem Klick auf *Berechtigungen* können Sie die Berechtigungen für lokale Gruppen, lokale Benutzer, Domänengruppen oder Domänenbenutzer festlegen.



Abbildung 8.8 Erweiterte Freigabe

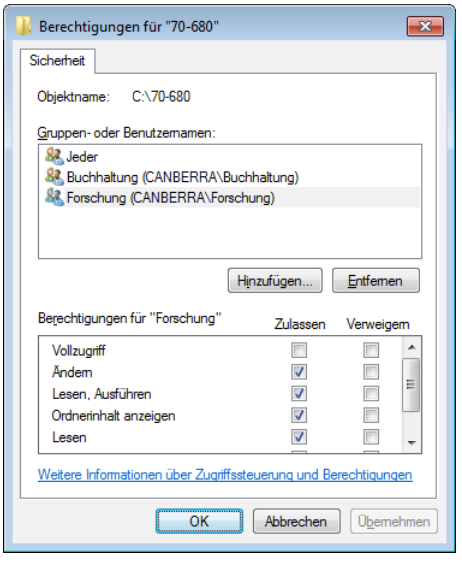


Abbildung 8.9 Erweiterte Berechtigungen

Wie Sie in Abbildung 8.9 sehen, werden die Berechtigungen zwar anders benannt als im einfachen Dialogfeld *Dateifreigabe*, sie bieten aber dieselbe Funktionalität. Die Berechtigung *Lesen* ermöglicht einem Benutzer oder einer Gruppe den Zugriff auf eine Datei oder einen Ordner, aber nicht die Änderung oder Löschung. Die Berechtigung *Ändern* umfasst nicht nur die Berechtigung *Lesen*, sondern auch das Hinzufügen, Löschen und Ändern von Dateien aus dem freigegebenen Ordner. Diese Berechtigung lässt sich mit der Berechtigung *Lesen/Schreiben* aus einem einfachen Dialogfeld *Dateifreigabe* vergleichen. Die Berechtigung *Vollzugriff* umfasst alle Rechte der Berechtigungen *Ändern* und *Lesen*. Außerdem ermöglicht sie es einem Benutzer, die Berechtigungen von anderen Benutzern zu ändern. *Vollzugriff* entspricht der Berechtigung *Besitzer* aus dem einfachen Freigabedialogfeld, wobei allerdings mehrere Benutzer oder Gruppen über die Berechtigung *Vollzugriff* verfügen können, während es bei der einfachen Dateifreigabe nur einen *Besitzer* geben kann.

Wenn Sie im Dialogfeld *Erweiterte Freigabe* auf *Zwischenspeichern* klicken, öffnet sich das Dialogfeld *Offlineeinstellungen* (Abbildung 8.10). Die Offlineeinstellungen legen fest, ob Programme und Dateien aus freigegebenen Ordnern auch dann verfügbar sind, wenn der Computer, auf dem die Dateien liegen, nicht im Netzwerk verfügbar ist. Über Offlineeinstellungen erfahren Sie mehr in Kapitel 11, »BitLocker und Mobilitätsoptionen«.

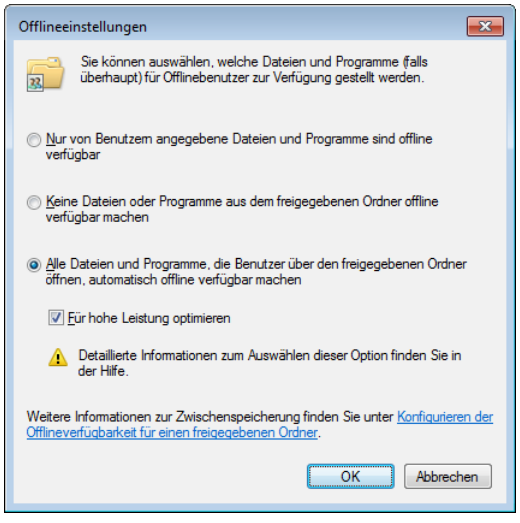

Offlineeinstellungen
Sie können auswählen, welche Dateien und Programme (falls überhaupt) für Offlinebenutzer zur Verfügung gestellt werden.
Nur von Benutzern angegebene Dateien und Programme sind offline verfügbar
Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen
Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen
Für hohe Leistung optimieren
Detaillierte Informationen zum Auswählen dieser Option finden Sie in der Hilfe.
Weitere Informationen zur Zwischenspeicherung finden Sie unter Konfigurieren der Offlineverfügbarkeit für einen freigegebenen Ordner.
OK
Abbrechen

Abbildung 8.10 Offlineeinstellungen für freigegebene Ordner

Im Knoten *Freigegebene Ordner* der Konsole *Computerverwaltung* können Sie alle freigegebenen Ordner eines Windows 7-Computers zentral verwalten. Unter dem Knoten *Freigaben* werden alle freigegebenen Ordner des Computers angezeigt (Abbildung 8.11). Der Knoten *Sitzungen* liefert Informationen darüber, welche Remotebenutzer aktuell mit dem freigegebenen Ordner verbunden sind, woher die Verbindung stammt und wie lange sie bereits besteht. Der Knoten *Geöffnete Dateien* zeigt an, welche Ordner und Dateien Remotebenutzer verwenden. Sie können die Eigenschaften einer vorhandenen Freigabe bearbeiten, indem Sie sie in dieser Konsole mit der rechten Maustaste anklicken und *Eigenschaften* wählen. Um einen neuen freigegebenen Ordner zu erstellen, können Sie den Knoten *Freigaben* mit der rechten Maustaste anklicken und dann auf *Neue Freigabe* klicken. Dadurch

wird der Assistent zum Erstellen von Ordnerfreigaben gestartet. In einer Übung am Ende dieser Lektion erstellen Sie mit diesem Assistenten einen neuen freigegebenen Ordner.

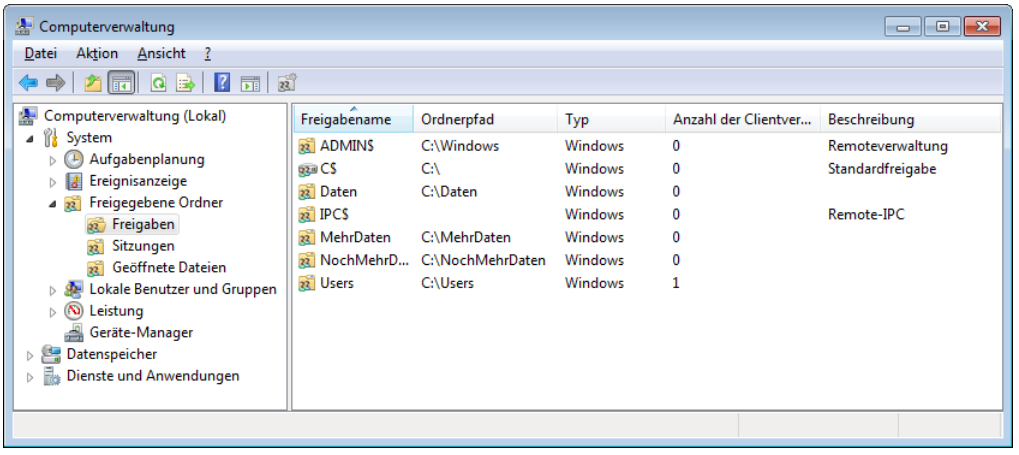


Abbildung 8.11 Anzeigen von Freigaben

Der Befehl `net share` ermöglicht die Verwaltung freigegebener Ordner auf der Befehlszeile. Diesen Befehl können Sie in Skripts verwenden, um die Erstellung von freigegebenen Ordnern auf Windows 7-Computern zu automatisieren. Verwenden Sie zur Erstellung eines freigegebenen Ordners folgenden Befehl:

```
net share Freigabename=Laufwerk:Pfad
```

Für die Zuweisung von Berechtigungen für den freigegebenen Ordner verwenden Sie folgenden Befehl:

```
net share Freigabename /grant:Benutzer Read/Change/Full
```

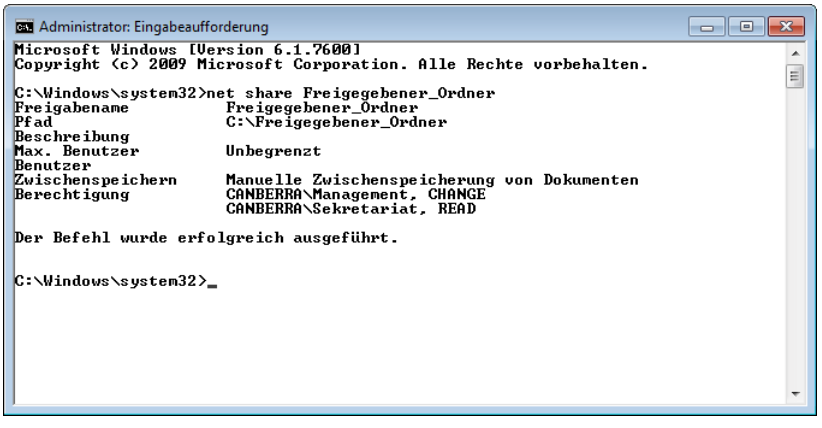


Abbildung 8.12 Eigenschaften eines freigegebenen Ordners

Mit dem Befehl `net share` können Sie auch die Zwischenspeicherung konfigurieren und die Zahl der Benutzer beschränken, die gleichzeitig Zugriff auf den freigegebenen Ordner erhalten. Zur Anzeige der Eigenschaften eines freigegebenen Ordners können Sie, wie in Abbildung 8.12 gezeigt, folgenden Befehl verwenden:

```
net share Freigabename
```

Zur Anzeige aller freigegebenen Ordner und der dazugehörigen Pfade verwenden Sie den Befehl `net share` ohne Optionen.



Weitere Informationen Freigabeberechtigungen und NTFS-Berechtigungen

Freigabe- und NTFS-Berechtigungen sind bei der Ermittlung der Berechtigungen eines Remotebenutzers beide wirksam. Über NTFS-Berechtigungen und die resultierenden Berechtigungen erfahren Sie mehr in Lektion 2, »Ordner- und Dateizugriff«.

Schnelltest

- Mit welchem Tool können Sie überprüfen, welche Ordner und Dateien Remotebenutzer auf einem Windows 7-Computer verwenden, auf dem Ordner freigegeben sind?

Antwort zum Schnelltest

- Im Knoten *Freigegebene Ordner\Geöffnete Dateien* der Konsole *Computerverwaltung* können Sie auf einem Windows 7-Computer überprüfen, welche Ordner und Dateien von Remotebenutzern verwendet werden.

Bibliotheken

Eine *Bibliothek* ist eine virtualisierte Sammlung von Ordnern. Sie ist also kein Ordner irgendwo auf der Festplatte der Unterordner enthält, sondern eine Sammlung von Verknüpfungen zu vorhandenen Ordnern. Wenn Sie in einer Eingabeaufforderung in den Ordner *Libraries* wechseln, werden Sie feststellen, dass er Dateien mit der Namensendung *.library-ms* enthält (Abbildung 8.13). Diese Dateien enthalten die Verknüpfungen mit den Ordnern. Jede dieser Dateien ist eine separate Bibliothek.

Bibliotheken machen es möglich, Ordner, die lokal und im Netzwerk an den verschiedensten Stellen gespeichert sind, bei der Darstellung im Windows-Explorer an einem einzigen Ort zusammenzufassen. Sie können zum Beispiel die Bibliothek *Dokumente* so einrichten, dass sie Dokumentordner von anderen Computern aus der Heimnetzgruppe sowie andere Ordner vom lokalen Festplattenlaufwerk des Computers enthält. Bibliotheken müssen nicht auf bestimmte Dateitypen beschränkt sein. Allerdings ist es besser, sie auf bestimmte Inhalte zu beschränken, um die Navigation zu vereinfachen.

Wenn Sie zu einer vorhandenen Bibliothek weitere Ordner hinzufügen möchten, klicken Sie im Eigenschaftendialogfeld der Bibliothek auf *Ordner hinzufügen* (Abbildung 8.14). Im selben Eigenschaftendialogfeld können Sie Ordner aus einer Bibliothek entfernen. Wenn Sie eine neue Bibliothek erstellen möchten, klicken Sie in der Strukturansicht des Windows-Explorers den Knoten *Bibliotheken* an und wählen *Neue Bibliothek*. In einer Übung am Ende dieser Lektion erstellen Sie eine neue Bibliothek.

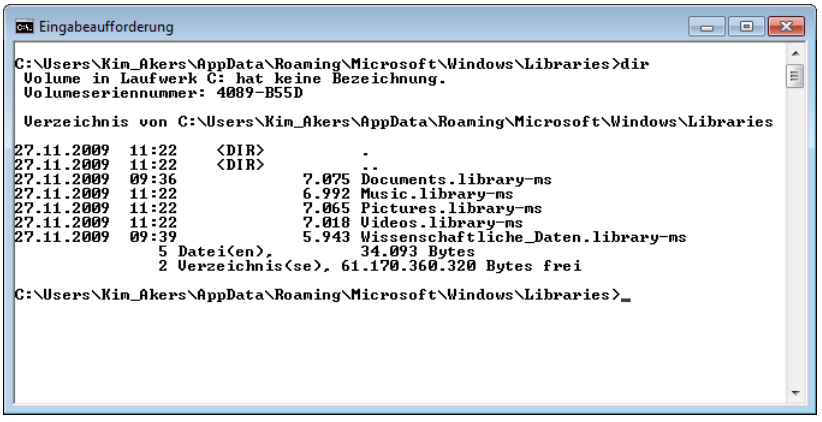


Abbildung 8.13 Der Ordner *Libraries* in einer Eingabeaufforderung

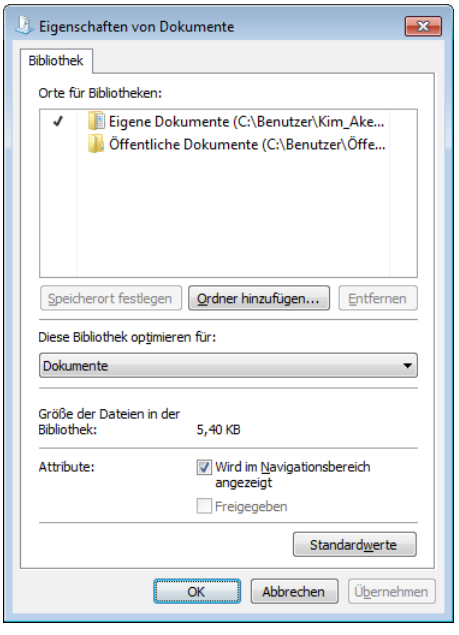


Abbildung 8.14 Speicherorte einer Bibliothek

Freigeben von Druckern

Freigegebene Drucker ermöglichen es Benutzern, Dokumente an einen Drucker zu senden, der im Netzwerk an einem anderen Windows 7-Computer angeschlossen ist. Zur Freigabe eines Druckers aktivieren Sie die Druckerfreigabe in der Heimnetzgruppe oder in den erweiterten Freigabeeinstellungen und suchen den Drucker dann auf der Seite *Geräte und Drucker* der Systemsteuerung heraus. Klicken Sie den Drucker, den Sie freigeben möchten, mit der rechten Maustaste an. Klicken Sie auf *Druckereigenschaften*, dann auf die Registerkarte *Freigabe* und aktivieren Sie dann das Kontrollkästchen *Drucker freigeben* (Abbildung 8.15). Wenn Sie einen Drucker für ältere Windows-Versionen freigeben, können Sie mit *Zusätzliche Treiber* die gewünschten Druckertreiber hinzufügen, damit andere Computer

im Netzwerk, auf denen die Treiber nicht installiert sind, die Treiber von dem Computer herunterladen können, auf dem der Drucker freigegeben wird.

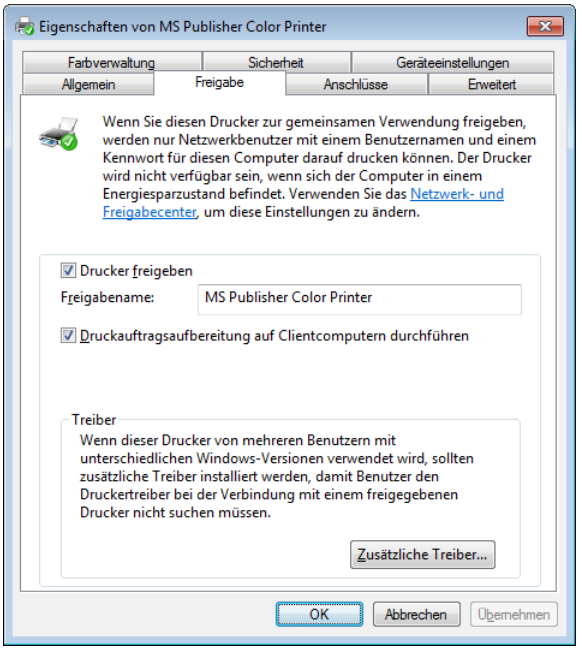

Eigenschaften von MS Publisher Color Printer
Farbverwaltung
Sicherheit
Geräteeinstellungen
Allgemein
Freigabe
Anschlüsse
Erweitert
Wenn Sie diesen Drucker zur gemeinsamen Verwendung freigeben, werden nur Netzwerkbenutzer mit einem Benutzernamen und einem Kennwort für diesen Computer darauf drucken können. Der Drucker wird nicht verfügbar sein, wenn sich der Computer in einem Energiesparzustand befindet. Verwenden Sie das Netzwerk- und Freigabecenter, um diese Einstellungen zu ändern.
Drucker freigeben
Freigabename:
MS Publisher Color Printer
Druckauftragsaufbereitung auf Clientcomputern durchführen
Treiber
Wenn dieser Drucker von mehreren Benutzern mit unterschiedlichen Windows-Versionen verwendet wird, sollten zusätzliche Treiber installiert werden, damit Benutzer den Druckertreiber bei der Verbindung mit einem freigegebenen Drucker nicht suchen müssen.
Zusätzliche Treiber...
OK
Abbrechen
Übernehmen

Abbildung 8.15 Druckerfreigabeoptionen

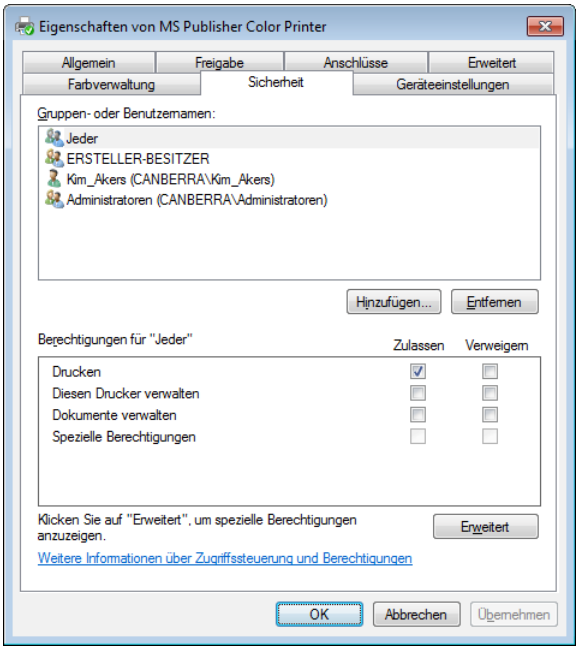


Abbildung 8.16 Sicherheitseinstellungen für die Druckerfreigabe

Bei der Freigabe eines Druckers erhält die Gruppe *Jeder* standardmäßig die Berechtigung *Drucken* (Abbildung 8.16). Das bedeutet, dass alle Mitglieder der Heimnetzgruppe oder im Fall einer Domänenumgebung jeder Benutzer, der Mitglied der Domäne ist, Druckaufträge an den Drucker senden kann. Wenn mehrere Leute den Drucker verwenden, können Sie versuchen, die Druckerverwaltung mit einer der drei folgenden Berechtigungen zu verbessern:

- **Drucken** Diese Berechtigung erlaubt es einem Benutzer, auf dem Drucker zu drucken und die Reihenfolge der Dokumente zu ändern, die er an den Drucker gesendet hat.
- **Diesen Drucker verwalten** Benutzer mit der Berechtigung *Diesen Drucker verwalten* können den Drucker anhalten und neu starten, die Einstellungen der Druckerwarteschlange ändern, Druckerberechtigungen und Druckereigenschaften ändern und einen Drucker freigeben.
- **Dokumente verwalten** Diese Berechtigung ermöglicht es Benutzern oder Gruppen, den Drucker anzuhalten oder weiterlaufen zu lassen, Dokumente aus der Druckerwarteschlange zu entfernen und die Reihenfolge der von Benutzern übermittelten Dokumente in der Druckerwarteschlange zu ändern.



Weitere Informationen Verwalten von Druckerberechtigungen

Weitere Informationen über die Verwaltung von Druckerberechtigungen finden Sie im TechNet auf folgender Seite: *http://technet.microsoft.com/de-de/library/cc773372(WS.10).aspx.*



Prüfungstipp

Merken Sie sich, welche Berechtigungen Sie einer Gruppe zuweisen müssen, damit Mitglieder dieser Gruppe zwar ihre eigenen Dokumente, aber nicht die Dokumente anderer Benutzer verwalten können, die an einen freigegebenen Drucker übermittelt wurden.

Übung Freigeben von Ressourcen

Statt einen Dateiserver bereitzustellen, verwenden viele kleinere Firmen für den Austausch von Dokumenten freigegebene Ordner, die auf den Arbeitsstationen eingerichtet werden. In dieser Übung verwenden Sie für den Datenaustausch die integrierten Funktionen von Windows 7 für Heimnetzgruppen und einige freigegebene Ordner.

Übung 1 Konfigurieren der Bibliotheken und der Heimnetzgruppe

In dieser Übung erstellen Sie eine neue Bibliothek und geben sie dann frei. Außerdem ändern Sie das Kennwort für die Heimnetzgruppe, damit es für die anderen Benutzer aus der Heimnetzgruppe leichter zu merken ist.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Erstellen Sie mit dem Windows-Explorer die Ordner *C:\Daten*, *C:\MehrDaten* und *C:\NochMehrDaten*.
3. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Bibliotheken** ein. Klicken Sie dann im *Start*-Menü auf Bibliotheken. Es öffnet sich der virtuelle Ordner *Bibliotheken* (Abbildung 8.17).
4. Klicken Sie auf *Neue Bibliothek*. Es wird eine neue Bibliothek erstellt. Geben Sie ihr den Namen **Wissenschaftliche_Daten**.

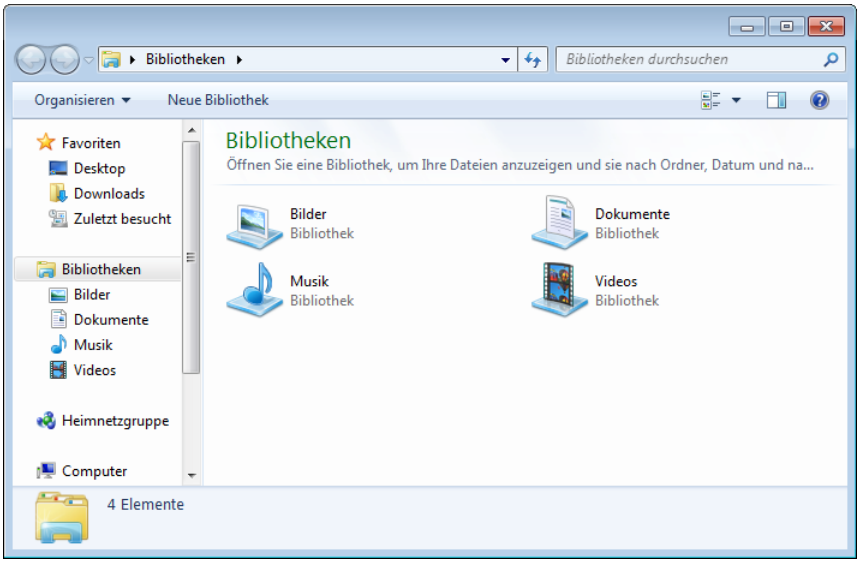


Abbildung 8.17 Der virtuelle Ordner *Bibliotheken*

5. Klicken Sie den Ordner *Wissenschaftliche_Daten* mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Dadurch öffnet sich das Dialogfeld *Eigenschaften von Wissenschaftliche_Daten*. Klicken Sie auf *Ordner hinzufügen*, suchen Sie den Ordner *C:\Daten* heraus und klicken Sie auf *Ordner aufnehmen*. Wiederholen Sie dies mit den Ordnern *C:\MehrDaten* und *C:\NochMehrDaten*.

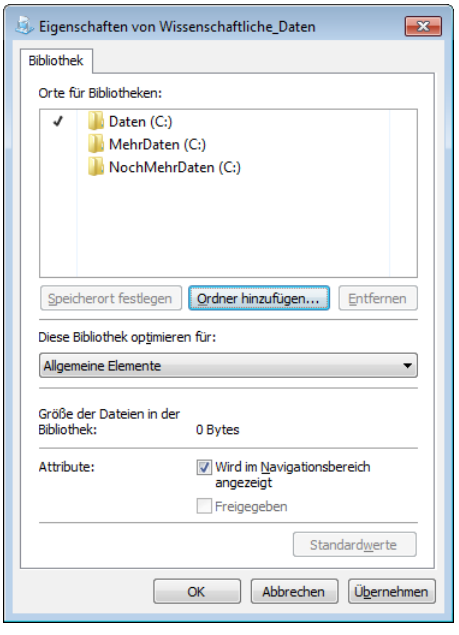


Abbildung 8.18 Eigenschaften der Bibliothek

6. Überprüfen Sie das Dialogfeld *Eigenschaften von Wissenschaftliche_Daten* anhand von Abbildung 8.18 und klicken Sie dann auf *OK*.
7. Klicken Sie die Bibliothek *Wissenschaftliche_Daten* mit der rechten Maustaste an, wählen Sie *Freigeben für* und klicken Sie dann auf *Heimnetzgruppe (Lesen)*.
8. Falls sich das Dialogfeld *Dateifreigabe* öffnet (Abbildung 8.19), klicken Sie auf *Ja, die Elemente freigeben*.

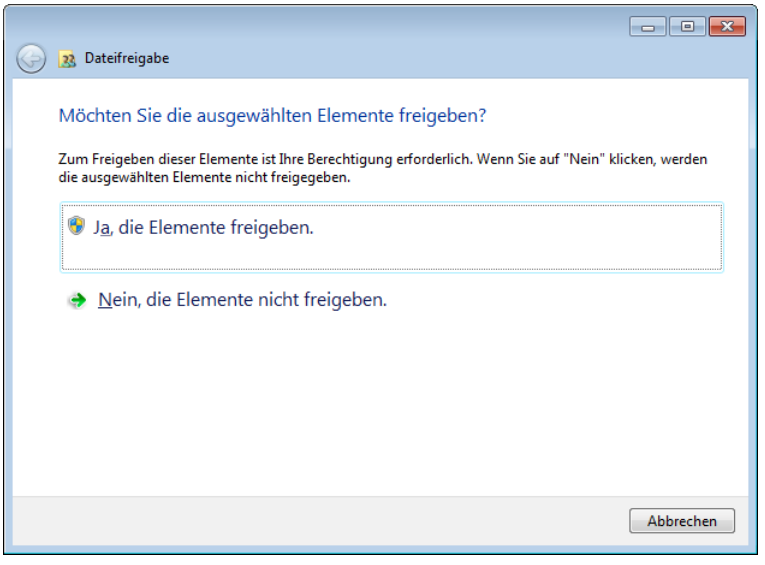

Dateifreigabe
Möchten Sie die ausgewählten Elemente freigeben?
Zum Freigeben dieser Elemente ist Ihre Berechtigung erforderlich. Wenn Sie auf "Nein" klicken, werden die ausgewählten Elemente nicht freigegeben.
Ja, die Elemente freigeben.
Nein, die Elemente nicht freigeben.
Abbrechen

Abbildung 8.19 Elemente freigeben

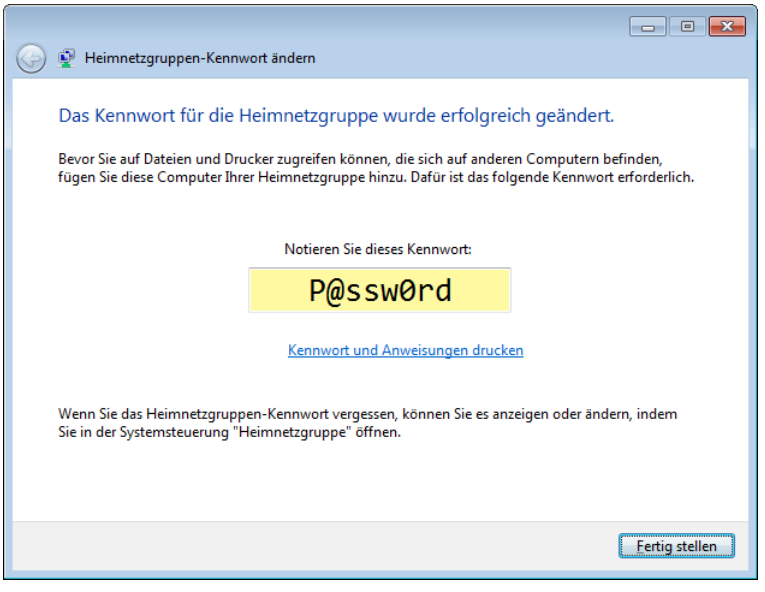

Heimnetzgruppen-Kennwort ändern
Das Kennwort für die Heimnetzgruppe wurde erfolgreich geändert.
Bevor Sie auf Dateien und Drucker zugreifen können, die sich auf anderen Computern befinden, fügen Sie diese Computer Ihrer Heimnetzgruppe hinzu. Dafür ist das folgende Kennwort erforderlich.
Notieren Sie dieses Kennwort:
P@ssw0rd
Kennwort und Anweisungen drucken
Wenn Sie das Heimnetzgruppen-Kennwort vergessen, können Sie es anzeigen oder ändern, indem Sie in der Systemsteuerung "Heimnetzgruppe" öffnen.
Fertig stellen

Abbildung 8.20 Das Kennwort für die Heimnetzgruppe wurde geändert

9. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Heimnetzgruppe** ein**.** Klicken Sie dann im *Start*-Menü auf den Eintrag *Heimnetzgruppe*. Es öffnet sich die Seite *Heimnetzgruppe* der Systemsteuerung.
10. Klicken Sie auf *Kennwort ändern*. Klicken Sie auch im Dialogfeld *Heimnetzgruppen-Kennwort ändern* auf *Kennwort ändern*.
11. Geben Sie auf der Seite *Geben Sie ein neues Kennwort für Ihre Heimnetzgruppe ein* das Kennwort **P@ssw0rd** ein und klicken Sie auf *Weiter*.
12. Überprüfen Sie das Kennwort für Ihre Heimnetzgruppe anhand von Abbildung 8.20 und klicken Sie dann auf *Fertig stellen*.

Übung 2 Erweiterte Ordnerfreigabe

In dieser Übung verwenden Sie zur Freigabe eines Ordners den Assistenten zum Erstellen von Ordnerfreigaben. Diese Methode sollten Sie wählen, wenn Ihr Computer mit einem Domänennetzwerk verbunden ist. Dann können Sie die Funktionen der Heimnetzgruppe nämlich nicht verwenden, aber es ist möglich, Bibliotheken direkt freizugeben.

1. Falls Sie noch nicht angemeldet sind, melden Sie sich mit dem Benutzerkonto *Kim_Akers* am Computer *Canberra* an.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und verwenden Sie folgende Befehle:

```
Net localgroup Management /add
Net localgroup Sekretariat /add
Mkdir c:\Freigegebener_Ordner
```

3. Geben Sie **exit** ein, um die Eingabeaufforderung zu schließen.
4. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Computerverwaltung** ein**.** Klicken Sie dann im *Start*-Menü auf *Computerverwaltung*. Dadurch öffnet sich die Konsole *Computerverwaltung*.
5. Erweitern Sie den Knoten *System\Freigegebene Ordner*. Klicken Sie den Knoten *Freigaben* mit der rechten Maustaste an und wählen Sie dann *Neue Freigabe*. Es wird der Assistent zum Erstellen von Ordnerfreigaben gestartet. Klicken Sie auf *Weiter*.
6. Geben Sie im Textfeld *Ordnerpfad* den Pfad **C:\Freigegebener_Ordner** ein (Abbildung 8.21) und klicken Sie dann auf *Weiter*.
7. Übernehmen Sie auf der Seite *Name, Beschreibung und Einstellungen* mit einem Klick auf *Weiter* die Standardeinstellungen.
8. Wählen Sie auf der Seite *Berechtigungen für freigegebene Ordner* die Option *Berechtigungen anpassen* und klicken Sie dann auf *Benutzerdefiniert*.
9. Wählen Sie auf der Registerkarte *Freigabeberechtigungen* die Gruppe *Jeder* und klicken Sie dann auf *Entfernen*. Klicken Sie auf *Hinzufügen*. Geben Sie im Dialogfeld *Benutzer oder Gruppen auswählen* **Management; Sekretariat** ein und klicken Sie dann auf *OK*.
10. Geben Sie der Gruppe *Sekretariat* die Berechtigung zum Lesen und der Gruppe *Management* die Berechtigung zum Ändern (Abbildung 8.22). Klicken Sie auf *OK*.

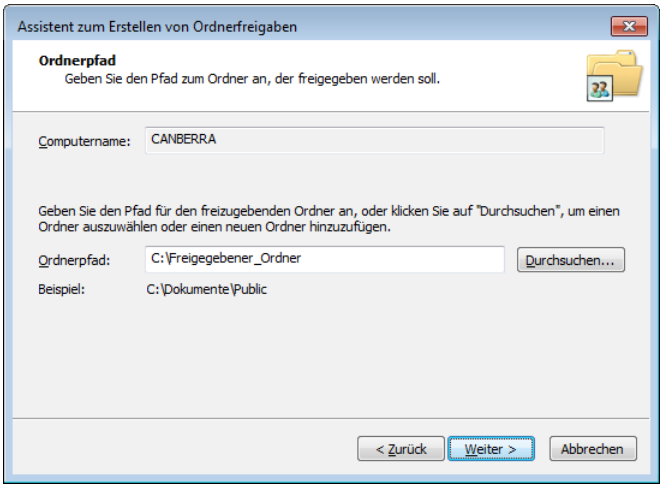

Assistent zum Erstellen von Ordnerfreigaben
Ordnerpfad
Geben Sie den Pfad zum Ordner an, der freigegeben werden soll.
Computername:
CANBERRA
Geben Sie den Pfad für den freizugebenden Ordner an, oder klicken Sie auf "Durchsuchen", um einen Ordner auszuwählen oder einen neuen Ordner hinzuzufügen.
Ordnerpfad:
C:\Freigegebener_Ordner
Durchsuchen...
Beispiel:
C:\Dokumente\Public
< Zurück
Weiter >
Abbrechen

Abbildung 8.21 Angeben des Pfads des freizugebenden Ordners

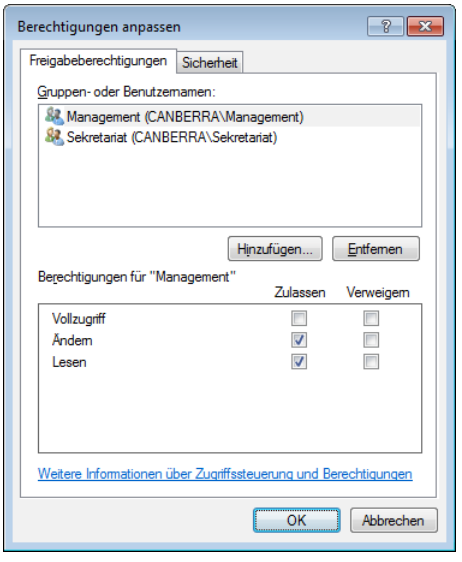


Abbildung 8.22 Benutzerdefinierte Freigabeberechtigungen

11. Klicken Sie zweimal auf *Fertig stellen*, um den Assistenten zum Erstellen von Ordnerfreigaben zu schließen.
12. Verwenden Sie in einer Eingabeaufforderung mit erhöhten Rechten den Befehl **net share Freigegebener_Ordner**, um zu überprüfen, ob die Gruppe *Management* die Berechtigung zum Ändern und die Gruppe *Sekretariat* die Berechtigung zum Lesen erhalten hat.

Zusammenfassung der Lektion

- Heimnetzgruppen können in Netzwerken eingerichtet werden, die als Heimnetzwerke konfiguriert wurden. Sie erleichtern in Umgebungen ohne AD DS die gemeinsame Verwendung von Ressourcen.
- Bibliotheken sind Sammlungen von Ordnern. Sie können Bibliotheken für eine Heimnetzgruppe freigeben.
- Auch einzelne Ordner lassen sich freigeben. Die Freigabeoptionen für Ordner gehen etwas mehr ins Detail als die Freigabeoptionen für Bibliotheken.
- Freigegebene Ordner können Sie mit der Konsole *Computerverwaltung*, mit Windows-Explorer und dem Befehl `net share` verwalten. Die Konsole *Computerverwaltung* ermöglicht die zentrale Verwaltung der freigegebenen Ordner.
- Die Druckerberechtigung *Drucken* ermöglicht Benutzern die Kontrolle ihrer eigenen Dokumente. Die Berechtigung *Dokumente verwalten* ermöglicht Benutzern die Verwaltung aller Dokumente, die an den Drucker übermittelt wurden. Die Druckerberechtigung *Diesen Drucker verwalten* ermöglicht Benutzern die Verwaltung der Druckereinstellungen und die Konfiguration der Druckerberechtigungen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Freigeben von Ressourcen«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie sind für die Verwaltung eines Computers zuständig, der mit Windows 7 Enterprise in einem Universitätslabor verwendet wird und mit vier verschiedenen wissenschaftlichen Instrumenten verbunden ist. Jedes dieser Instrumente speichert seine Daten in einem Verzeichnis namens *Daten*. Die Datenverzeichnisse der verschiedenen Instrumente liegen auf verschiedenen Volumes des Festplattenlaufwerks des Computers. Sie möchten diese Daten mithilfe der gemeinsamen Heimnetzgruppe auf anderen Computern des Labors verfügbar machen. Was sollten Sie tun? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)
   A. Sie geben jeden Datenordner frei.
   B. Sie erstellen eine Bibliothek namens *Wissenschaftliche_Daten*.
   C. Sie fügen die separaten Datenordner der Instrumente zur Bibliothek *Wissenschaftliche_Daten* hinzu.
   D. Sie geben die Bibliothek *Wissenschaftliche_Daten* auf der Seite *Heimnetzgruppe* der Systemsteuerung frei.

2. Sie beraten ein kleines Geschäft, das einen Farblaserdrucker besitzt. Der Drucker ist an dem Windows 7-Computer des Assistenten der Geschäftsleitung angeschlossen. Der Assistent ist kein Mitglied der lokalen Gruppe *Administratoren*. Sie möchten, dass der Assistent Druckaufträge in der Warteschlange anders anordnen und sie bei Bedarf löschen kann. Der Assistent sollte dies mit allen Dokumenten tun können, die sich in der Druckerwarteschlange befinden. Er sollte aber nicht in der Lage sein, die Druckerberechtigungen zu ändern. Wie erreichen Sie dieses Ziel?
   A. Sie weisen dem Assistenten die Berechtigung *Drucken* zu.
   B. Sie geben dem Assistenten die Berechtigung *Diesen Drucker verwalten*.
   C. Sie weisen dem Assistenten die Berechtigung *Dokumente verwalten* zu.
   D. Sie fügen das Konto des Assistenten zur Gruppe *Hauptbenutzer* hinzu.
3. Mit welchen der folgenden Tools können Sie überprüfen, welche freigegebenen Ordner es auf einem Windows 7-Computer gibt und welche lokalen Ordner diesen Freigaben zugeordnet sind? (Wählen Sie alle zutreffenden Antworten.)
   A. Befehl `net share`
   B. Konsole *Computerverwaltung*
   C. Bibliotheken
   D. Netzwerk- und Freigabecenter
4. Sie haben auf einem Windows 7-Computer eine lokale Gruppe namens *Buchhaltung* erstellt. Welche der folgenden Freigabeberechtigungen sollten Sie dieser Gruppe zuweisen, damit ihre Mitglieder Dateien zum freigegebenen Buchhaltungsordner hinzufügen und sie ändern oder löschen können, ohne den Mitgliedern dieser Gruppe die Möglichkeit zu geben, Freigabeberechtigungen zu ändern?
   A. *Lesen*
   B. *Ändern*
   C. *Vollzugriff*
   D. *Besitzer*
5. Welche der folgenden erweiterten Freigabeeinstellungen sollten Sie konfigurieren, damit freigegebene Ressourcen auf einem Windows 7-Computer für alle anderen Computer aus der Heimnetzgruppe sichtbar werden?
   A. *Freigabe des öffentlichen Ordners*
   B. *Dateifreigabeverbindungen*
   C. *Kennwortgeschütztes Freigeben*
   D. *Netzwerkerkennung*

Lektion 2: Ordner- und Dateizugriff

In vielen Windows 7-Bereitstellungen müssen mehrere Leute denselben Computer verwenden. Wenn mehrere Leute abwechselnd am selben Computer arbeiten und ihre Dateien lokal speichern, ist es notwendig, dafür zu sorgen, dass ein Benutzer nur dann die Dateien eines anderen Benutzers einsehen kann, wenn er über die entsprechenden Berechtigungen verfügt. Windows 7 ermöglicht dies durch Datei- und Ordnerberechtigungen sowie durch eine Verschlüsselung mit dem verschlüsselnden Dateisystem (Encrypting File System, EFS)

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren von Datei- und Ordnerberechtigungen
- Beheben von Problemen mit den effektiven Berechtigungen
- Verschlüsseln von Dateien und Ordnern

Veranschlagte Zeit für diese Lektion: 40 Minuten

Datei- und Ordnerberechtigungen

Sie können NTFS-Datei- und Ordnerberechtigungen einzelnen Benutzerkonten oder Gruppen zuweisen. NTFS-Datei- und Ordnerberechtigungen bestimmen die Zugriffsrechte auf Dateien und Ordner. Diese Zugriffsrechte gelten unabhängig davon, ob sich der Benutzer direkt am Windows 7-Computer anmeldet oder über das Netzwerk auf den Computer zugreift. Datei- und Ordnerberechtigungen können Sie nur für Dateien und Ordner auf NTFS-Volumes festlegen. Es ist nicht möglich, Datei- und Ordnerberechtigungen für Dateien und Ordner auf FAT- oder FAT32-Volumes festzulegen.

Es gibt sechs Standardberechtigungen, die einer Datei oder einem Ordner zugewiesen werden können:

- **Vollzugriff** Auf Ordner angewendet, ermöglicht diese Berechtigung das Lesen, Schreiben, Ändern und Löschen von Dateien und Unterordnern. Auf eine Datei angewendet, erlaubt sie das Lesen, Schreiben, Ändern und Löschen der Datei. Lässt auch die Änderung von Berechtigungen für Dateien und Ordnern zu.
- **Ändern** Wird sie auf Ordner angewendet, erlaubt diese Berechtigung das Lesen, Schreiben, Ändern und Löschen von Dateien und Unterordnern. Auf eine Datei angewendet, lässt sie das Lesen, Schreiben, Ändern und Löschen der Datei zu. Erlaubt keine Änderung der Berechtigungen für Dateien und Ordner.
- **Lesen, Ausführen** Auf Ordner angewendet, lässt diese Berechtigung den Zugriff auf den Inhalt des Ordners und die Ausführung von ausführbaren Dateien zu. Auf eine Datei angewendet, erlaubt Sie den Zugriff auf die Datei und die Ausführung der Datei.
- **Ordnerinhalt anzeigen** Kann nur auf Ordner angewendet werden und erlaubt die Anzeige des Ordnerinhalts.
- **Lesen** Erlaubt, auf Ordner angewendet, den Zugriff auf den Inhalt. Auf eine Datei angewendet, lässt diese Berechtigung den Zugriff auf die Datei zu. Der Unterschied zu *Lesen, Ausführen* besteht darin, dass Dateien nicht ausgeführt werden können.
- **Schreiben** Auf Ordner angewendet, ermöglicht diese Berechtigung das Hinzufügen von Dateien und Unterordnern. Wird sie auf eine Datei angewendet, kann ein Benutzer die Datei ändern, aber sie nicht löschen.

Um diese Berechtigungen einem Benutzer oder einer Gruppe zuzuweisen, öffnen Sie das Eigenschaftendialogfeld des fraglichen Ordners oder der Datei und klicken auf die Registerkarte *Sicherheit*. Sie können die Berechtigungen mit der Einstellung *Zulassen* oder *Verweigern* zuweisen. Verweigerte Berechtigungen haben immer Vorrang vor zugelassenen Berechtigungen. Wird eine Berechtigung nicht ausdrücklich für einen Benutzer zugelassen, verfügt der Benutzer nicht über diese Berechtigung und kann die entsprechenden Arbeiten nicht durchführen.

Wie Abbildung 8.23 zeigt, verfügt die Benutzerin Kim Akers über die Berechtigungen *Lesen, Ausführen (Zulassen)*, *Ordnerinhalt anzeigen (Zulassen)* und *Lesen (Zulassen)* für den Ordner *Temp*. Andere Berechtigungen wie *Ändern* wurden nicht eingestellt. Sofern sie die Berechtigung *Ändern (Zulassen)* nicht durch eine Gruppenmitgliedschaft erhält, kann Kim Akers Dateien im Ordner *Temp* nicht ändern.

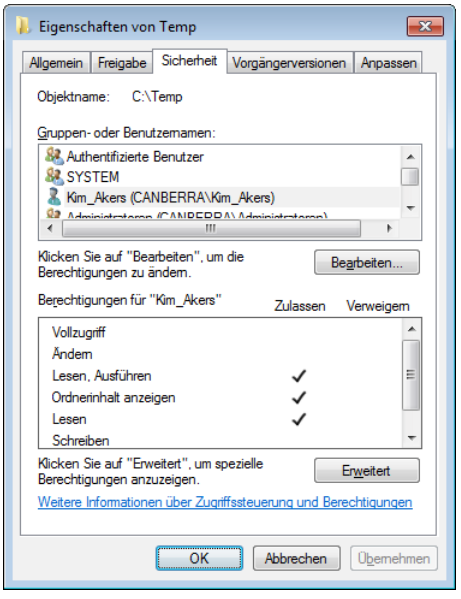


Abbildung 8.23 Standardberechtigungen

Bei der Zulassung bestimmter Berechtigungen werden auch andere Berechtigungen automatisch mit eingeschlossen. Wenn Sie zum Beispiel die Berechtigung *Lesen, Ausführen (Zulassen)* einstellen, fügt Windows automatisch die Berechtigungen *Ordnerinhalt anzeigen (Zulassen)* und *Lesen (Zulassen)* hinzu. Auch die Verweigerung einer bestimmten Berechtigung kann andere Berechtigungen einschließen. Tabelle 8.1 beschreibt, welche Berechtigungen bei der Zuweisung einer bestimmten Berechtigung ebenfalls zugewiesen werden.

Tabelle 8.1 Berechtigungen und darin eingeschlossene Berechtigungen

Berechtigung	Darin eingeschlossene Berechtigungen
Vollzugriff	*Vollzugriff*; *Ändern*; *Lesen, Ausführen*; *Ordnerinhalt anzeigen*; *Lesen*; *Schreiben*
Ändern	*Ändern*; *Lesen, Ausführen*; *Ordnerinhalt anzeigen*; *Lesen*; *Schreiben*
Lesen, Ausführen	*Lesen, Ausführen*; *Ordnerinhalt anzeigen*; *Lesen*
Ordnerinhalt anzeigen	*Ordnerinhalt anzeigen*
Lesen	*Lesen*
Schreiben	*Schreiben*

Schnelltest

1. Welche zusätzlichen Berechtigungen werden bei der Zuweisung von *Ändern (Zulassen)* zugewiesen?
2. Welche Berechtigung sollten Sie zuweisen, wenn ein Benutzer den Inhalt einer Datei ändern, die Datei aber nicht löschen können soll?

Antworten zum Schnelltest

1. Wenn Sie die Berechtigung *Ändern (Zulassen)* zuweisen, fügt Windows automatisch die Berechtigungen *Lesen, Ausführen (Zulassen)*, *Ordnerinhalt anzeigen (Zulassen)*, *Lesen (Zulassen)* und *Schreiben (Zulassen)* hinzu.
2. Die Berechtigung *Schreiben* ermöglicht einem Benutzer die Änderung des Dateiinhalts, aber nicht das Löschen der Datei.

Spezielle Berechtigungen

Die sechs NTFS-Berechtigungen setzen sich jeweils aus mehreren speziellen Berechtigungen zusammen. Deswegen werden auch andere Berechtigungen automatisch mit eingeschlossen, wenn Sie Berechtigungen wie *Ändern* oder *Lesen, Ausführen* zuweisen. Die Gruppe der speziellen Berechtigungen, die bei der Zuweisung von *Lesen, Ausführen* verwendet wird, enthält auch die Berechtigungen, aus denen sich die Berechtigungen *Ordnerinhalt anzeigen* und *Lesen* zusammensetzen. In den meisten Fällen reichen die sechs NTFS-Berechtigungen aus. Wenn sich ungewöhnliche Situationen ergeben, in denen Sie die Berechtigungen genauer anpassen müssen, können Sie die speziellen Berechtigungen ändern. Dazu klicken Sie auf der Registerkarte *Sicherheit* des Eigenschaftendialogfelds einer Datei oder eines Ordners auf die Schaltfläche *Erweitert*, wählen den Benutzer oder die Gruppe aus, klicken dann auf *Berechtigungen ändern* und schließlich auf *Bearbeiten*. Abbildung 8.24 zeigt das Dialogfeld *Berechtigungseintrag*.

Tabelle 8.2 zeigt die speziellen Berechtigungen, aus denen sich die sechs NTFS-Berechtigungen zusammensetzen. Die speziellen Berechtigungen zum Durchsuchen und Auflisten von Ordnern gelten nur für Ordner und nicht für einzelne Dateien. Die speziellen Berechtigungen werden hier nur der Vollständigkeit halber gezeigt. Es ist unwahrscheinlich, dass sie in der Prüfung 70-680 im Detail abgefragt werden.

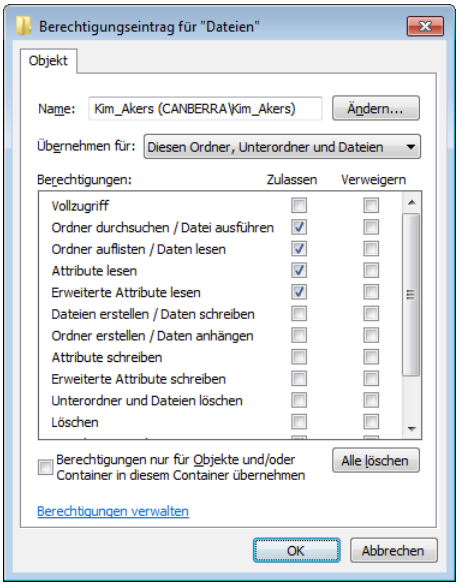


Abbildung 8.24 Spezielle Berechtigungen

Tabelle 8.2 Spezielle Berechtigungen und NTFS-Berechtigungen

Spezielle Berechtigung	Vollzugriff	Ändern	Lesen, Ausführen	Ordnerinhalt anzeigen	Lesen	Schreiben
Ordner durchsuchen/ Datei ausführen	X	X	X	X		
Ordner auflisten/ Daten lesen	X	X	X	X	X	
Attribute lesen	X	X	X	X	X	
Erweiterte Attribute lesen	X	X	X	X	X	
Dateien erstellen/ Daten schreiben	X	X				X
Ordner erstellen/ Daten anhängen	X	X				X
Attribute schreiben	X	X				X
Erweiterte Attribute schreiben	X	X				X
Unterordner und Dateien löschen	X					
Löschen	X	X				
Berechtigungen lesen	X	X	X	X	X	X
Berechtigungen ändern	X					
Besitz übernehmen	X					

Erben von Berechtigungen

Neu erstellte Dateien und Ordner erben die Berechtigungen des Ordners, in dem sie erstellt wurden. Gibt es zum Beispiel einen Ordner namens *Alpha*, für den der Gruppe *Entwicklung* die Berechtigung *Ändern (Zulassen)* zugewiesen wurde, erhält diese Gruppe standardmäßig auch für alle Dateien und Ordner, die im Ordner *Alpha* erstellt werden, die Berechtigung *Ändern (Zulassen)*.

Die Vererbung von Berechtigungen lässt sich ändern. Klicken Sie dazu im Eigenschaftendialogfeld der betreffenden Datei oder des Ordners auf *Erweitert*, dann auf *Berechtigungen ändern*, und löschen Sie die Option *Vererbbare Berechtigungen des übergeordneten Objektes einschließen* (Abbildung 8.25). Wenn Sie diese Option löschen, haben Sie die Wahl, die geerbten Berechtigungen zu entfernen oder zu übernehmen, damit sie für das Objekt gelten. Bei der Bearbeitung der erweiterten Sicherheitseinstellungen eines Ordners haben Sie auch die Option, die Berechtigungen aller untergeordneten Objekte durch die Berechtigung des bearbeiteten Objekts zu ersetzen.

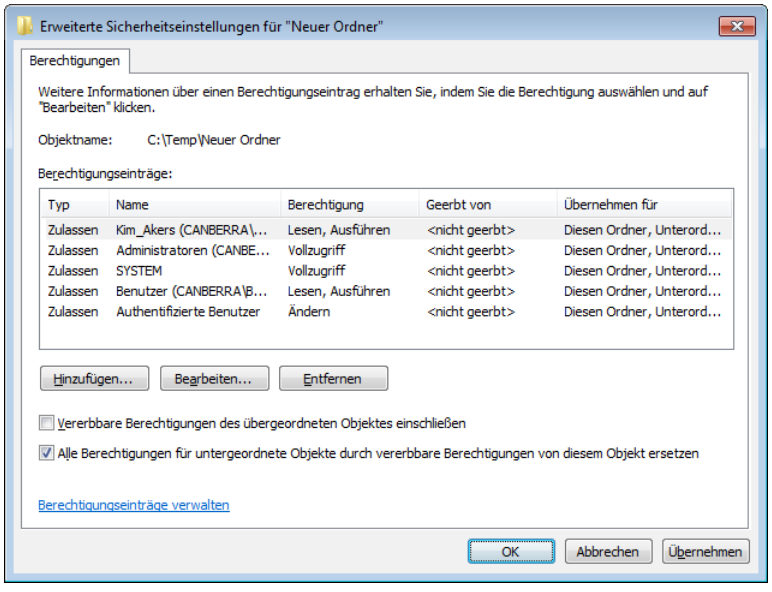

Erweiterte Sicherheitseinstellungen für "Neuer Ordner"
Berechtigungen
Weitere Informationen über einen Berechtigungseintrag erhalten Sie, indem Sie die Berechtigung auswählen und auf "Bearbeiten" klicken.
Objektname: C:\Temp\Neuer Ordner
Berechtigungseinträge:
Typ Name Berechtigung Geerbt von Übernehmen für
Zulassen Kim_Akers (CANBERRA\... Lesen, Ausführen <nicht geerbt> Diesen Ordner, Unterord...
Zulassen Administratoren (CANBE... Vollzugriff <nicht geerbt> Diesen Ordner, Unterord...
Zulassen SYSTEM Vollzugriff <nicht geerbt> Diesen Ordner, Unterord...
Zulassen Benutzer (CANBERRA\B... Lesen, Ausführen <nicht geerbt> Diesen Ordner, Unterord...
Zulassen Authentifizierte Benutzer Ändern <nicht geerbt> Diesen Ordner, Unterord...
Hinzufügen... Bearbeiten... Entfernen
Vererbbare Berechtigungen des übergeordneten Objektes einschließen
Alle Berechtigungen für untergeordnete Objekte durch vererbbare Berechtigungen von diesem Objekt ersetzen
Berechtigungseinträge verwalten
OK Abbrechen Übernehmen

Abbildung 8.25 Einstellung der Vererbung von Berechtigungen

Konfigurieren von Berechtigungen mit Icacls

Icacls ist ein Befehlszeilenprogramm, mit dem Sie auf einem Windows 7-Computer die NTFS-Berechtigungen von Dateien und Ordnern anzeigen und konfigurieren können. Zur Anzeige der Berechtigungen einer Datei oder eines Ordners können Sie den Befehl `Icacls` *`Datei_oder_Ordner`* verwenden. Für die Zuweisung von Berechtigungen verwenden Sie die Syntax `Icacls` *`Datei_oder_Ordner`* `/grant` *`Benutzer_oder_Gruppe:Berechtigung`*. Mit der Option `/deny` legen Sie Berechtigungsablehnungen statt Zulassungen fest. Folgende NTFS-Berechtigungen können Sie zuweisen:

- F (Full Control, *Vollzugriff*)
- M (Modify, *Ändern*)

- RX (Read, Execute, *Lesen, Ausführen*)
- R (Read, *Lesen*)
- W (Write, *Schreiben*)

Wollen Sie zum Beispiel dem Benutzerkonto *Kim_Akers* für den Ordner *C:\Buchhaltung* die NTFS-Berechtigung *Ändern* zuweisen, verwenden Sie den Befehl

```
Icacls.exe C:\Buchhaltung /grant Kim_Akers:(OI)M
```

Um dem Benutzerkonto *Kim_Akers* die Berechtigung *Lesen, Ausführen (Verweigern)* für den Ordner *C:\Forschung* zuzuweisen, verwenden Sie den Befehl

```
Icacls.exe C:\Forschung /deny Kim_Akers:(OI)RX
```

Icacls lässt sich auch zur Speicherung und Wiederherstellung der Berechtigungen von Dateien und Ordnern verwenden. Um alle NTFS-Berechtigungen des Ordners *C:\Test* und seiner Unterordner in einer Datei namens *Berechtigungen* zu speichern, verwenden Sie den Befehl

```
Icacls C:\Test\* /save Berechtigungen /t
```

Mit der Option `/restore` können Sie die Berechtigungen wiederherstellen. Die Möglichkeit zur Speicherung und Wiederherstellung von Berechtigungen kann sich zum Beispiel als nützlich erweisen, wenn Sie Dateien und Ordner auf andere Volumes kopieren. In einer Übung am Ende dieser Lektion weisen Sie mit Icacls Berechtigungen zu.



Weitere Informationen Icacls

Weitere Informationen über die Syntax und Optionen von Icacls, einschließlich der Verwendung spezieller Berechtigungen, finden Sie in folgendem TechNet-Dokument: *http://technet.microsoft.com/en-us/library/cc753525(WS.10).aspx*.

Ermitteln der effektiven Berechtigungen

Ist ein Benutzer Mitglied mehrerer Gruppen und wurden diesen Gruppen für denselben Ordner unterschiedliche Berechtigungen zugewiesen, lässt sich nur schwer erkennen, über welche Berechtigungen der Benutzer tatsächlich verfügt. Berechtigungen sind kumulativ und Berechtigungsverweigerungen haben Vorrang vor Zulassungen. Verfügen verschiedene Gruppen über mehrere Berechtigungszulassungen, können die Verhältnisse sehr unübersichtlich werden. Wenn Sie bei der Bestimmung der Berechtigungen, über die ein Benutzer tatsächlich verfügt, die Gruppenmitgliedschaften nicht berücksichtigen, werden Sie nicht zum richtigen Ergebnis kommen.

Auf der Registerkarte *Effektive Berechtigungen* können Sie ermitteln, über welche Berechtigungen für eine Datei oder einen Ordner ein Benutzer oder eine Gruppe tatsächlich verfügt. Die Registerkarte *Effektive Berechtigungen* analysiert die Berechtigungen eines Benutzers und die Berechtigungen aller Gruppen, denen er angehört, um zu bestimmen, welche Berechtigungen für das fragliche Objekt wirksam (effektiv) sind. Um die Registerkarte *Effektive Berechtigungen* zu öffnen, klicken Sie auf der Registerkarte *Sicherheit* aus dem Eigenschaftendialogfeld der Datei oder des Ordners auf die Schaltfläche *Erweitert* und wählen die Registerkarte *Effektive Berechtigungen*. Klicken Sie auf *Auswählen*, um die Gruppe oder den Benutzer auszuwählen, dessen effektive Berechtigungen Sie ermitteln möchten (Abbildung 8.26). In einer Übung am Ende dieser Lektion bestimmen Sie die effektiven Berechtigungen eines Benutzers.

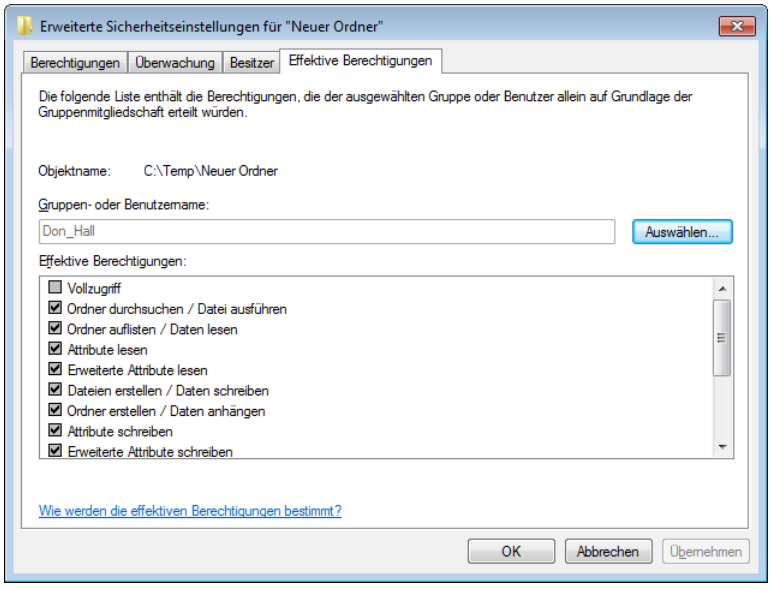


Abbildung 8.26 Ermitteln der effektiven Berechtigungen

Kopieren und Verschieben von Dateien

Berechtigungen werden beim Kopieren einer Datei, beim Verschieben einer Datei an einen anderen Ort auf demselben Volume und beim Verschieben einer Datei auf ein anderes Volume unterschiedlich behandelt. Dieselben Vererbungsregeln, die beim Kopieren oder Verschieben einer Datei gelten, gelten auch beim Kopieren oder Verschieben von Ordnern.

Wenn Sie eine Datei von einem Ordner in einen anderen verschieben, erbt die Datei die Berechtigungen des Zielordners. Diese Regel gilt unabhängig davon, ob Sie die Datei in einen anderen Ordner desselben Volumes oder auf ein anderes Volume kopieren. Wenn Sie zum Beispiel den Mitgliedern der Gruppe *Forschung* für den Ordner *Alpha* die Berechtigung *Schreiben (Verweigern)* zugewiesen haben und für den Ordner *Beta* die Berechtigung *Ändern (Zulassen)*, erhalten Mitglieder der Gruppe *Forschung* für jede Datei, die von *Alpha* nach *Beta* kopiert wird, die Berechtigung *Ändern (Zulassen)*. Die Regeln, die beim Kopieren von Dateien gelten, gelten auch für das Kopieren von Ordnern. Wenn Sie einen Ordner von einem übergeordneten Ordner in einen anderen kopieren, erben der Ordner und alle darin enthaltenen Ordner die Berechtigungen des Zielordners.

Welche Regeln bei der Verschiebung von Dateien aus einem Ordner in einen anderen gelten, hängt davon ab, ob der Zielordner auf demselben Volume oder auf einem anderen liegt. Wenn Sie eine Datei zwischen Ordnern desselben Volumes verschieben, behält die Datei ihre ursprünglichen Berechtigungen. Haben Sie zum Beispiel den Mitgliedern der Gruppe *Forschung* die Berechtigung *Schreiben (Verweigern)* für den Ordner *Alpha* und die Berechtigung *Ändern (Zulassen)* für den Ordner *Beta* zugewiesen und verschieben eine Datei vom Ordner *Alpha* in den Ordner *Beta*, behält die Gruppe *Forschung* ihre ursprüngliche Berechtigung *Schreiben (Verweigern)* für diese Datei. Dasselbe gilt, wenn Sie einen Ordner verschieben. Die Berechtigungen für den Ordner und seinen Inhalt bleiben erhalten, wenn er auf demselben Volume an einen anderen Ort verschoben wird.

Wenn Sie eine Datei von einem Ordner in einen anderen verschieben, der auf einem anderen Volume liegt, verhält sie sich so, als wäre sie in den Zielordner kopiert worden und würde die Berechtigungen des Zielordners erben. Das gilt auch für einen Ordner. Wenn Sie einen Ordner von einem Volume auf ein anderes verschieben, erben dieser Ordner und sein Inhalt die Berechtigungen des Zielordners.

RoboCopy.exe ist ein Befehlszeilenprogramm von Windows 7, mit dem Sie Dateien mit ihren NTFS-Berechtigungen kopieren können. Sie können *RoboCopy.exe* auch verwenden, um Dateien mit ihren NTFS-Berechtigungen von einem Volume auf ein anderes zu verschieben. Betrachten Sie *RoboCopy.exe* als Ausnahme von den Regeln für das Kopieren und Verschieben von Dateien. In der Prüfung sollten Sie die normalen Regeln voraussetzen, solange in der Fragestellung nicht von *RoboCopy.exe* die Rede ist. Um alle Dateien und Ordner aus dem Ordner *C:\Beispiel* mit *RoboCopy.exe* in den Ordner *D:\Ziel* zu verschieben, verwenden Sie den Befehl

```
RoboCopy.exe C:\Beispiel D:\Ziel /copyall /e
```



Hinweis Verschieben von Dateien und Ordnern auf FAT-Volumes

Wenn Sie eine Datei oder einen Ordner auf ein Volume verschieben, das mit dem Dateisystem FAT oder FAT32 formatiert ist, gehen alle NTFS-Berechtigungen verloren.

Kombinierte Freigabe- und NTFS-Berechtigungen

Wenn ein Benutzer auf eine Datei zugreift, die in einem freigegebenen Ordner liegt, gelten die Freigabeberechtigungen, die bereits in Lektion 1 besprochen wurden, und die NTFS-Berechtigungen. Zur Wirkung kommt jeweils die am stärksten einschränkende Berechtigung. Wurde einer Gruppe zum Beispiel auf der Freigabeebene die Berechtigung *Lesen* zugewiesen und in den Datei- und Ordnerberechtigungen die Berechtigung *Ändern*, erhält der Benutzer nur Lesezugriff auf die Dateien und Ordner, wenn er über das Netzwerk eine Verbindung mit dem freigegebenen Ordner herstellt. Verfügt ein Benutzer auf Freigabeebene über die Berechtigung *Vollzugriff* und in den NTFS-Berechtigungen nur über die Berechtigung *Lesen*, erhält er nur Lesezugriff und kann keine Dateien und Ordner aus der Freigabe löschen.

Konfigurieren der Überwachung

Sie können überwachen, welche Benutzer und Gruppen auf bestimmte Dateien und Ordner zugreifen. Wahrscheinlich werden Sie nicht sämtliche Zugriffe auf alle Dokumente Ihrer Organisation überwachen, sondern nur Zugriffe auf sensible Dokumente. Vielleicht würden Sie zum Beispiel Zugriffe auf die Kalkulationstabelle mit den Gehältern der Angestellten überwachen, aber nicht Zugriffe auf den Putzplan für den Pausenraum. Durch die Überwachung erfahren Sie, wer ein Dokument geöffnet hat, wer es geändert hat und wer vergeblich versucht hat, es zu öffnen. Sie können die Verwendung aller speziellen Berechtigungen überwachen, die in Tabelle 8.2 aufgeführt werden. Eine Überwachung ist allerdings nur auf Volumes möglich, die mit dem NTFS-Dateisystem formatiert sind.

Die Überwachungsrichtlinien von Windows 7 ermöglichen eine genauere Konfiguration der Überwachungsereignisse als in den älteren Windows-Versionen. Unter Windows XP konnten Sie zum Beispiel 9 umfangreiche Ereigniskategorien überwachen. Windows 7 bietet 53 verschiedene Ereigniskategorien. Dadurch lassen sich die zu überwachenden Ereignisse genauer eingrenzen. So können Sie unter Windows 7 den Benutzerzugriff auf bestimmte Dateien und Ordner überwachen:

1. Öffnen Sie den Editor für lokale Gruppenrichtlinien und suchen Sie den Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen* heraus. Stellen Sie die Richtlinie *Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen (Windows Vista oder höher), um Kategorieeinstellungen der Überwachungsrichtlinie außer Kraft zu setzen* auf *Aktiviert*.
2. Wechseln Sie im Editor für lokale Gruppenrichtlinien zu dem Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Systemüberwachungsrichtlinien – Lokales Gruppenrichtlinienobjekt\Objektzugriff* und aktivieren Sie die Richtlinie *Dateisystem überwachen* (Abbildung 8.27).

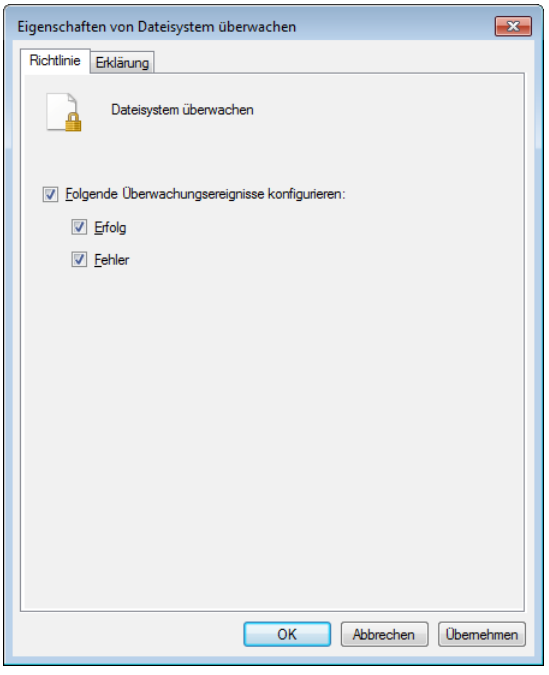


Abbildung 8.27 Konfigurieren von Überwachungsrichtlinien

3. Öffnen Sie das Eigenschaftendialogfeld der zu überwachenden Datei oder des zu überwachenden Ordners. Klicken Sie auf der Registerkarte *Sicherheit* auf *Erweitert*, dann auf die Registerkarte *Überwachung* und schließlich auf die Schaltfläche *Fortsetzen*, um die Berechtigungen anzuheben.
4. Klicken Sie auf *Hinzufügen* und fügen Sie die Gruppen hinzu, deren Zugriffe Sie überwachen möchten. Wenn Sie die Zugriffe aller Benutzer überwachen möchten, wählen Sie die Gruppe *Jeder*. Nachdem Sie die Sicherheitsgruppe gewählt haben, müssen Sie festlegen, welche Rechteverwendung Sie überwachen möchten. Abbildung 8.28 zeigt eine Konfiguration zur Überwachung erfolgreicher Schreib- und Lesezugriffe sowie Löschungen.
5. Die Überwachungsereignisse werden nun im Sicherheitsprotokoll erfasst, das Sie in der Ereignisanzeige einsehen können.

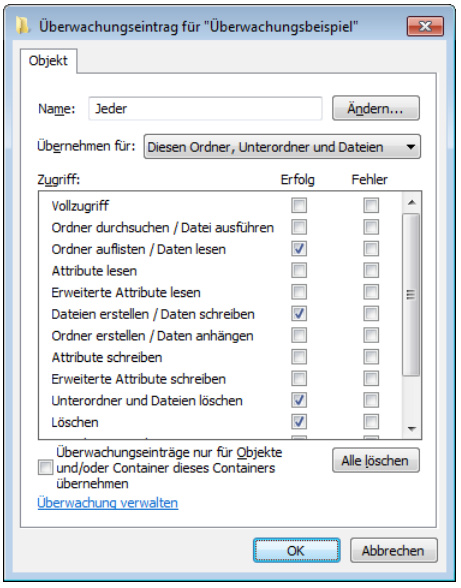


Abbildung 8.28 Konfiguration der zu überwachenden Rechteverwendung



Weitere Informationen **Erweiterte Überwachungsrichtlinien**

Weitere Informationen über die erweiterten Überwachungsoptionen von Windows 7 finden Sie in der folgenden Schritt-für-Schritt-Anleitung im TechNet: *http://technet.microsoft.com/de-de/library/dd408940(WS.10).aspx*.

Schnelltest

- Behalten ein Ordner und sein Inhalt ihre ursprünglichen NTFS-Berechtigungen bei, wenn Sie den Ordner auf demselben Volume an einen anderen Ort verschieben?

Antwort zum Schnelltest

- Ja. Wenn Dateien oder Ordner auf demselben Volume an einen anderen Ort verschoben werden, behalten sie ihre ursprünglichen NTFS-Berechtigungen.

Verschlüsselndes Dateisystem

Das *verschlüsselnde Dateisystem* (Encrypting File System, EFS) ist in den Editionen Professional, Enterprise und Ultimate von Windows 7 verfügbar und ermöglicht Ihnen die Verschlüsselung von einzelnen Dateien und Ordnern. EFS unterscheidet sich von BitLocker To Go, weil BitLocker ganze Volumes verschlüsselt und nicht direkt auf der Ebene von Dateien und Ordnern arbeitet. Sie können BitLocker beispielsweise zur Verschlüsselung eines USB-Flashlaufwerks (Universal Serial Bus) verwenden, nachdem Sie es an einen Windows 7-Computer angeschlossen haben. Dabei werden alle Dateien und Ordner des Laufwerks verschlüsselt, weil das gesamte Volume verschlüsselt wird. Allerdings haben alle Benutzer des Windows 7-Computers Zugriff auf die Dateien, die auf diesem USB-Flashlaufwerk gespeichert sind, solange sie nicht durch strenge Einstellungen der Berechtigungen daran gehindert werden, weil das Volume nicht für einen speziellen Benutzer, sondern für

den Windows 7-Computer verschlüsselt wird. EFS ermöglicht es, die auf dem USB-Flashlaufwerk gespeicherten Dateien und Ordner für bestimmte Benutzerkonten des Windows 7-Computers zu verschlüsseln. Die EFS-Verschlüsselung bewirkt, dass auch ein Benutzer, der über Lesezugriff auf die Datei verfügt, die Datei nicht öffnen kann, wenn er nicht über das erforderliche Verschlüsselungszertifikat verfügt. Über BitLocker erfahren Sie mehr in Kapitel 11.

EFS verwendet eine *Verschlüsselung mit öffentlichem Schlüssel* (Public Key Encryption). Bei diesem Verfahren verfügt ein Benutzer über zwei Schlüssel, nämlich über einen öffentlichen und über einen privaten (geheimen) Schlüssel. Der öffentliche Schlüssel wird in Form eines Zertifikats im Zertifikatspeicher des Computers gespeichert und ist jedermann zugänglich. Benutzer können den öffentlichen Schlüssel zur Verschlüsselung von Daten verwenden. Der private Schlüssel wird im privaten Zertifikatspeicher des Benutzers gespeichert und kann nur vom Benutzer verwendet werden. Mit dem privaten Schlüssel lassen sich Daten entschlüsseln, die mit dem öffentlichen Schlüssel verschlüsselt wurden. Wenn ein Benutzer das erste Mal auf einem Windows 7-Computer eine Datei verschlüsselt, erstellt der Windows 7-Computer ein EFS-Zertifikat und einen privaten Schlüssel.



Weitere Informationen So funktioniert EFS

Dateien werden nur indirekt mit EFS-Zertifikaten verschlüsselt. Zur Verschlüsselung einer Datei oder eines Ordners wird ein Dateiverschlüsselungsschlüssel (File Encryption Key, FEK) verwendet, der wiederum mit dem EFS-Zertifikat verschlüsselt wird. Jede Datei verfügt über ihren eigenen FEK. Statt eine Datei mehrfach zu verschlüsseln, wenn sie mit mehreren Schlüsseln verschlüsselt werden muss, wird sie nur einmal verschlüsselt. Der FEK wird aber entsprechend oft verschlüsselt, mit jedem EFS-Schlüssel einmal. Jeder Benutzer, der die verschlüsselte Datei verwendet, entschlüsselt den FEK mit seinem privaten Schlüssel und entschlüsselt die Datei dann mit dem FEK. Weitere Informationen über die Arbeitsweise von EFS finden Sie im TechNet unter: *http://technet.microsoft.com/en-us/library/cc962103.aspx*.

Mit EFS können Sie nur Dateien verschlüsseln, die auf NTFS-Volumes gespeichert sind. Da die meisten USB-Flashlaufwerke mit einem FAT32-Volume geliefert werden, müssen Sie die Laufwerke also zuerst mit NTFS formatieren, bevor Sie EFS-verschlüsselte Dateien und Ordner darauf speichern können. Der Windows-Explorer zeigt verschlüsselte Dateien und Ordner nicht in der üblichen schwarzen Schrift an, sondern grün.

Wenn Sie einen Ordner verschlüsseln, verschlüsselt Windows alle Dateien, die Sie in diesen Ordner kopieren oder darin erstellen. EFS ist nicht mit der Komprimierung von Dateien und Ordnern vereinbar. Wenn Sie eine Datei verschlüsseln, die in einem komprimierten Ordner liegt, wird die Datei zuerst dekomprimiert und bleibt dekomprimiert, solange sie verschlüsselt ist. Wenn Sie eine verschlüsselte Datei in einen komprimierten Ordner kopieren, bleibt die Datei verschlüsselt. Wenn Sie eine komprimierte Datei in einen verschlüsselten Ordner kopieren, wird die Datei dekomprimiert und verschlüsselt. Wenn Sie eine Datei oder einen Ordner mit EFS-Verschlüsselung auf ein FAT32-Volume kopieren, entschlüsselt Windows 7 die Datei oder den Ordner automatisch, wenn er/sie auf das Zielvolume geschrieben wird.

Mit EFS können Sie einzelne Dateien für mehrere Benutzer verschlüsseln. Wenn Sie das tun, können nur Benutzer, für die diese Dateien verschlüsselt wurden, die Datei lesen. Andere Benutzer können die Datei auch dann nicht lesen, wenn sie über die entsprechenden NTFS-

Berechtigungen verfügen, weil die Datei verschlüsselt ist. Allerdings können sie eine Datei nur dann für einen anderen Benutzer verschlüsseln, wenn im Zertifikatspeicher ein EFS-Zertifikat für diesen Benutzer vorliegt. Wenn Sie eine Datei für einen anderen Benutzer verschlüsseln wollen, dessen Zertifikat aber nicht finden können, müssen Sie den Benutzer dazu bringen, sich am Computer anzumelden und eine Datei zu verschlüsseln. Dabei wird ein EFS-Zertifikat für ihn erstellt, das anschließend im Zertifikatspeicher zu finden ist. Mit diesem Zertifikat können Sie Dateien für das Benutzerkonto dieses Benutzers verschlüsseln.

EFS ermöglicht zwar die Verschlüsselung einzelner Dateien für mehrere Benutzerkonten, aber nicht die Verschlüsselung von Ordnern für mehrere Benutzerkonten. Es ist auch nicht möglich, Dateien für Gruppen zu verschlüsseln. Das geht nur für mehrere einzelne Benutzer.



Hinweis EFS in Domänenumgebungen

Die Active Directory-Domänendienste (Active Directory Domain Services, AD DS) ermöglichen die zentrale Verwaltung von EFS-Zertifikaten in einer Domänenumgebung. Weil der Schwerpunkt in der Prüfung 70-680 aber auf eigenständigen Windows 7-Clientcomputern liegt, die keine Domänenmitglieder sind, brauchen Sie sich nicht mit der Integration von EFS in AD DS zu beschäftigen.

EFS-Wiederherstellung

Wiederherstellungsagenten sind Zertifikate, die eine Wiederherstellung von EFS-verschlüsselten Dateien ermöglichen. Wenn in den lokalen Gruppenrichtlinien ein Wiederherstellungsagent festgelegt wurde, können alle mit EFS verschlüsselten Dateien mit dem privaten Schlüssel des Wiederherstellungsagenten wiederhergestellt werden. Sie sollten den Wiederherstellungsagenten auf einem Windows 7-Computer festlegen, bevor Sie den Benutzern die Verschlüsselung von Dateien erlauben. Mit dem privaten Schlüssel des Wiederherstellungsagenten können Sie alle Dateien wiederherstellen, die nach der Festlegung des Wiederherstellungsagenten verschlüsselt wurden. Dateien, die vor der Installation eines Wiederherstellungsagentzertifikats verschlüsselt wurden, können Sie damit nicht wiederherstellen.

So erstellen Sie einen EFS-Wiederherstellungsagenten:

1. Melden Sie sich mit dem ersten Konto, das erstellt wurde, auf dem Windows 7-Computer an. Dieses Konto ist das Standardadministratorkonto.
2. Öffnen Sie eine Eingabeaufforderung und verwenden Sie den Befehl

   ```
   Cipher.exe /r:recoveryagent
   ```

3. Es werden zwei Dateien erstellt: *Recoveryagent.cer* und *Recoveryagent.pfx*. *Cipher.exe* fordert Sie zur Eingabe eines Kennworts auf, mit dem die Datei *Recoveryagent.pfx* geschützt wird.
4. Öffnen Sie den Editor für lokale Gruppenrichtlinien und navigieren Sie zum Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel\Verschlüsselndes Dateisystem*. Klicken Sie diesen Knoten mit der rechten Maustaste an und klicken Sie dann auf *Datenwiederherstellungs-Agents hinzufügen*. Geben Sie den Pfadnamen der Datei *Recoveryagent.cer* an oder suchen Sie diese Datei heraus, um dieses Zertifikat als Wiederherstellungsagenten festzulegen.
5. Importieren Sie die Datei *Recoveryagent.pfx* in der *Zertifikate*-Konsole, wenn Sie Dateien wiederherstellen möchten. Diese Datei enthält den privaten Schlüssel des

Wiederherstellungsagenten. Verwahren Sie die Datei an einem sicheren Ort, weil sich mit ihr alle Dateien öffnen lassen, die auf dem Windows 7-Computer mit EFS verschlüsselt wurden.

Sie können den Wiederherstellungsagenten auf einem zweiten Windows 7-Computer importieren, wenn Sie Dateien wiederherstellen möchten, die auf dem ersten Computer verschlüsselt wurden. Außerdem können Sie Dateien auf einem zweiten Windows 7-Computer wiederherstellen, indem Sie die EFS-Schlüssel vom ersten Computer exportieren und auf dem zweiten importieren. Zum Export und Import der EFS-Schlüssel eignet sich die *Zertifikate*-Konsole. Außerdem können Sie EFS-Schlüssel mit *Cipher.exe* sichern.

EFS und Heimnetzgruppen

Die gemeinsame Verwendung von EFS-verschlüsselten Dateien in Heimnetzumgebungen kann kompliziert werden, weil sie voraussetzt, dass jeder Computer aus der Heimnetzgruppe über dieselben EFS-Zertifikate verfügt. In Domänenumgebungen ist es möglich, EFS-Zertifikate zentral mit AD DS und den Active Directory-Zertifikatdiensten zu verwalten. In Heimnetzumgebungen gibt es keine zentrale Zertifikatverwaltung. Auch wenn ein Benutzer auf jedem Computer der Heimnetzgruppe denselben Kontonamen und dasselbe Kennwort verwendet, wird auf jedem Computer ein separates EFS-Zertifikat samt Schlüsselpaar erstellt.

Wenn Sie verschlüsselte Dateien in einer Heimnetzgruppe freigeben möchten, sollten Sie dafür sorgen, dass jeder Benutzer aus der Heimnetzgruppe auf einem Computer eine Datei verschlüsselt. Exportieren Sie dann mit der *Zertifikate*-Konsole oder mit dem Befehl *Cipher.exe* die EFS-Zertifikate samt Schlüssel auf ein USB-Flashlaufwerk. Die Zertifikate und Schlüssel sollten anschließend auf den anderen Windows 7-Computern aus der Heimnetzgruppe importiert werden.

Übung Verschlüsselung und Berechtigungen

EFS gab es zwar schon in mehreren älteren Windows-Versionen, aber nicht jeder Benutzer weiß, wie man eine Datei verschlüsselt. Selbst erfahrene Administratoren haben Schwierigkeiten damit, sich zu merken, welche NTFS-Dateiberechtigungen bei Dateiverschiebungen und Kopieraktionen bleiben und welche geerbt werden. In dieser Übung verschlüsseln Sie Dateien und überprüfen, wie sich NTFS-Berechtigungen durch Kopieraktionen und Dateiverschiebungen ändern.

Übung 1 Verschlüsseln einer einzelnen Datei für mehrere Benutzer

In dieser Übung erstellen Sie ein Textdokument und verschlüsseln es dann für zwei verschiedene Benutzerkonten. Da sich ein Dokument nur dann für ein Benutzerkonto verschlüsseln lässt, wenn das Konto über ein EFS-Zertifikat verfügt, ist es für diese Übung erforderlich, ein Dokument mit zwei verschiedenen Benutzerkonten zu verschlüsseln, bevor Sie ein Dokument für zwei Benutzer verschlüsseln können.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Öffnen Sie die Systemsteuerung und klicken Sie dann auf *Benutzerkonten hinzufügen/entfernen*.
3. Klicken Sie auf der Seite *Konten verwalten* auf *Neues Konto erstellen*. Geben Sie als Kontonamen **Jeff_Phillips** ein, wählen Sie den Typ *Standardbenutzer* und klicken Sie dann auf *Konto erstellen*.

4. Klicken Sie das Konto *Jeff_Phillips* auf der Seite *Konten verwalten* an und klicken Sie dann auf *Kennwort erstellen*. Geben Sie zweimal das Kennwort **P@ssw0rd** ein und verwenden Sie die Nummer dieser Buchseite als Kennworthinweis. Klicken Sie auf *Kennwort erstellen*. Schließen Sie die Systemsteuerung.
5. Klicken Sie den Desktop mit der rechten Maustaste an, klicken Sie auf *Neu* und dann auf *Ordner*. Nennen Sie den Ordner **Verschlüsselungstest** und öffnen Sie ihn.
6. Klicken Sie mit der rechten Maustaste in den Ordner, klicken Sie auf *Neu* und dann auf *Textdokument*. Nennen Sie das Dokument **Verschlüsseln.txt.** Öffnen Sie das Textdokument und geben Sie den Text **Konfigurieren von Windows 7** ein**.** Speichern und schließen Sie das Textdokument.
7. Klicken Sie die Datei *Verschlüsseln.txt* mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Klicken Sie auf der Registerkarte *Allgemein* des Dialogfelds *Eigenschaften von Verschlüsseln.txt* auf *Erweitert*. Wählen Sie im Dialogfeld *Erweiterte Attribute* das Kontrollkästchen *Inhalt verschlüsseln, um Daten zu schützen* (Abbildung 8.29). Klicken Sie auf *OK* und dann auf *Übernehmen*.

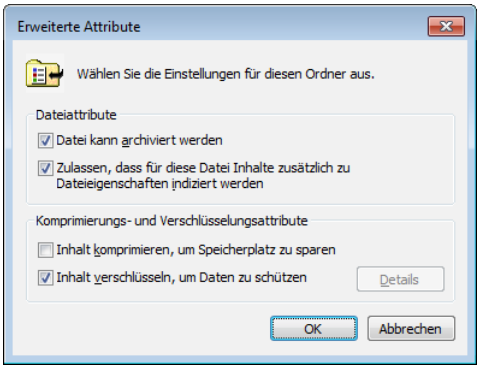

Erweiterte Attribute
Wählen Sie die Einstellungen für diesen Ordner aus.
Dateiattribute
Datei kann archiviert werden
Zulassen, dass für diese Datei Inhalte zusätzlich zu Dateieigenschaften indiziert werden
Komprimierungs- und Verschlüsselungsattribute
Inhalt komprimieren, um Speicherplatz zu sparen
Inhalt verschlüsseln, um Daten zu schützen
Details
OK
Abbrechen

Abbildung 8.29 Erweiterte Attribute

8. Wählen Sie im Dialogfeld *Verschlüsselungswarnung* das Kontrollkästchen *Nur Datei verschlüsseln* und klicken Sie dann auf *OK*. Die Datei ist nun verschlüsselt.
9. Klicken Sie auf der Registerkarte *Allgemein* des Dialogfelds *Eigenschaften von Verschlüsseln.txt* auf *Erweitert*. Klicken Sie im Dialogfeld *Erweiterte Attribute* auf *Details*. Klicken Sie im Dialogfeld *Benutzerzugriff auf Verschlüsseln.txt* auf *Hinzufügen*.
10. Überprüfen Sie im Dialogfeld *Windows-Sicherheit*, ob das einzige vorhandene Zertifikat auf *Kim_Akers* ausgestellt ist (Abbildung 8.30). Klicken Sie auf *OK*.
11. Klicken Sie im *Start*-Menü auf den Pfeil neben *Herunterfahren* und wählen Sie dann *Benutzer wechseln*.
12. Melden Sie sich mit dem Benutzerkonto *Jeff_Phillips* an.
13. Führen Sie die Schritte 5 bis 8 mit dem Benutzerkonto *Jeff_Phillips* durch und klicken Sie dann auf *OK*, um das Eigenschaftendialogfeld der Textdatei zu schließen.
14. Melden Sie sich als *Jeff_Phillips* ab und führen Sie die *Kim_Akers*-Sitzung fort. Das Dialogfeld *Benutzerzugriff auf Verschlüsseln.txt* sollte immer noch sichtbar sein, weil Sie die vorhandene Sitzung nicht beendet, sondern nur einen Benutzerwechsel durchgeführt haben.



Abbildung 8.30 EFS-Zertifikatauswahl

15. Klicken Sie im Dialogfeld *Benutzerzugriff auf Verschlüsseln.txt* auf *Hinzufügen*. Überprüfen Sie, ob im Dialogfeld *Windows-Sicherheit* nun zwei Verschlüsselungszertifikate angegeben werden. Klicken Sie das Zertifikat *Jeff_Phillips* an (Abbildung 8.31) und klicken Sie dann auf *OK*.

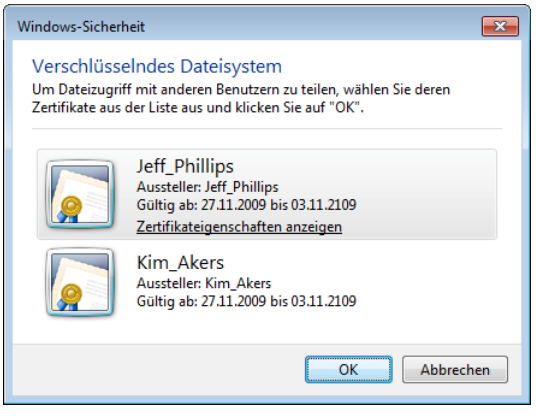


Abbildung 8.31 Ein weiteres EFS-Zertifikat ist verfügbar

16. Schließen Sie alle geöffneten Dialogfelder jeweils mit einem Klick auf *OK*.

Übung 2 Überprüfen von Datei- und Ordnerberechtigungen

In dieser Übung überprüfen Sie, wie sich Datei- und Ordnerberechtigungen ändern, wenn Sie Dateien zwischen zwei Ordnern kopieren oder verschieben. Als Tools verwenden Sie in dieser Übung Icacls und die Registerkarte *Effektive Berechtigungen*.

1. Sofern Sie es noch nicht getan haben, melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und verwenden Sie folgende Befehle:

```
net localgroup Forschung /add
net localgroup Buchhaltung /add
net localgroup Forschung Jeff_Phillips /Add
net localgroup Buchhaltung Jeff_Phillips /Add
```

```
mkdir C:\Quelle
mkdir C:\Ziel
icacls C:\Quelle /grant Forschung:(OI)(CI)M
icacls C:\Ziel /grant Buchhaltung:(OI)(CI)RX
icacls C:\Ziel /deny Jeff_Phillips:(OI)(CI)W
```

3. Öffnen Sie den Ordner *C:\Quelle* im Windows-Explorer. Klicken Sie mit der rechten Maustaste in den Ordner und erstellen Sie zwei neue Textdateien mit den Namen *Alpha* und *Beta*.
4. Klicken Sie *Alpha* mit der rechten Maustaste an und wählen Sie *Eigenschaften*. Klicken Sie auf die Registerkarte *Sicherheit* und dann auf die Gruppe *Forschung*. Überprüfen Sie die Berechtigungen anhand von Abbildung 8.32. Führen Sie dieselben Aktionen mit der Datei *Beta.txt* durch und überprüfen Sie, ob die Berechtigungen identisch sind.

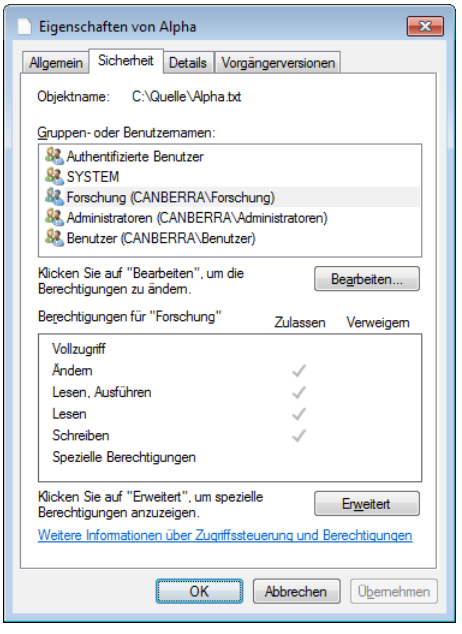


Abbildung 8.32 Berechtigungen für die Gruppe *Forschung* an *Alpha.txt*

5. Verwenden Sie in der Eingabeaufforderung folgende Befehle:

```
copy C:\Quelle\alpha.txt C:\Ziel
move C:\Quelle\beta.txt C:\Ziel
```

6. Vergleichen Sie die Eigenschaften der Datei *C:\Ziel\Alpha.txt* mit den Eigenschaften der Datei *C:\Ziel\Beta.txt*. Beachten Sie, dass *Beta.txt* noch dieselben Berechtigungen wie vor der Verschiebung aufweist, während sich die Berechtigungen für *Alpha.txt* geändert haben, insbesondere die Berechtigungen für die Gruppen *Forschung* und *Buchhaltung* und die Berechtigungen für den Benutzer *Jeff_Phillips* (Abbildung 8.33).

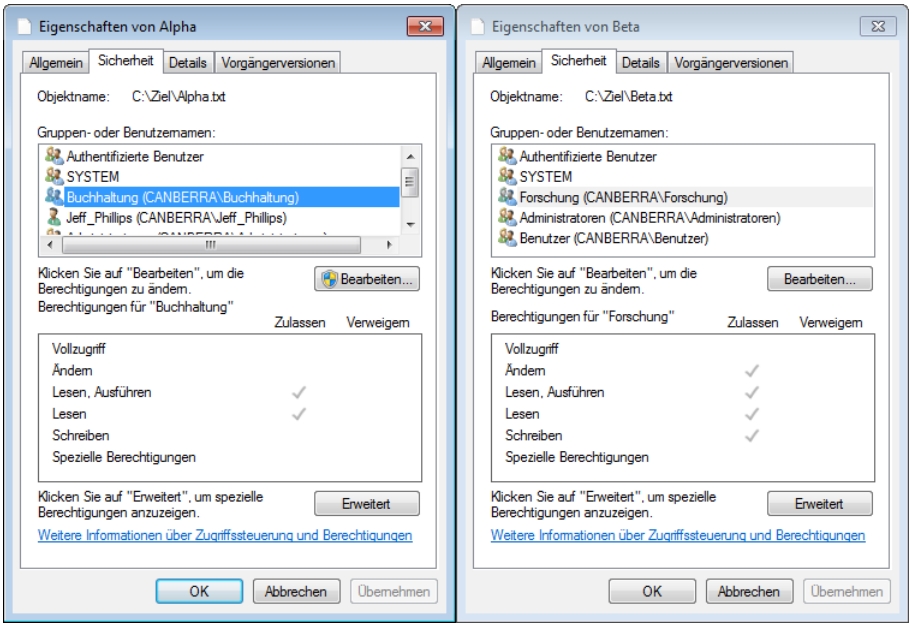


Abbildung 8.33 Vergleich der Berechtigungen

7. Klicken Sie im Eigenschaftendialogfeld der Datei *Alpha* auf die Registerkarte *Sicherheit* und dann auf *Jeff_Phillips*. Beachten Sie, dass das Konto *Jeff_Phillips* nur über die Berechtigung *Schreiben (Verweigern)* verfügt.
8. Klicken Sie auf *Erweitert*. Klicken Sie im Dialogfeld *Erweiterte Sicherheitseinstellungen* auf die Registerkarte *Effektive Berechtigungen*.

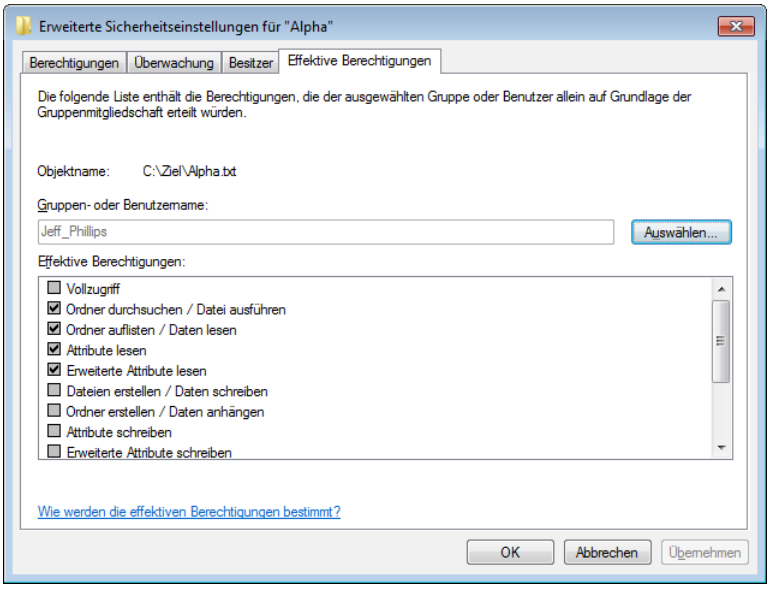


Abbildung 8.34 Ermittlung der effektiven Berechtigungen

9. Klicken Sie auf *Auswählen*. Es öffnet sich das Dialogfeld *Benutzer oder Gruppe auswählen*. Geben Sie den Namen **Jeff_Phillips** ein und klicken Sie dann auf *OK*. Überprüfen Sie die effektiven Berechtigungen des Benutzerkontos *Jeff_Phillips* (Abbildung 8.34). Die Berechtigungen weichen von den Berechtigungen ab, die dem Benutzerkonto zugewiesen wurden, weil auch die Berechtigungen aus der Gruppenmitgliedschaft zu berücksichtigen sind.

Zusammenfassung der Lektion

- Das Hilfsprogramm *Icacls.exe* eignet sich zur Verwaltung von NTFS-Berechtigungen auf der Befehlszeile.
- Es gibt sechs grundlegende NTFS-Berechtigungen: *Lesen*; *Schreiben*; *Ordnerinhalt anzeigen*; *Lesen, Ausführen*; *Ändern* und *Vollzugriff*. Eine Berechtigungsablehnung hat immer Vorrang vor einer Berechtigungszulassung.
- Auf der Registerkarte *Effektive Berechtigungen* können Sie die effektiven Berechtigungen eines Benutzers für eine Datei oder einen Ordner ermitteln. Das ist vor allem dann eine Arbeitserleichterung, wenn der Benutzer Mitglied mehrerer Gruppen ist, die über Berechtigungen für dieselbe Ressource verfügen.
- Bei der Kombination von Freigabe- und NTFS-Berechtigungen wird die am stärksten einschränkende Berechtigung wirksam.
- Zugriffe auf Dateien und Ordner lassen sich überwachen. Dadurch erfahren Sie, wer mit welchen Dateien und Ordnern gearbeitet hat oder arbeiten wollte.
- Wird eine Datei kopiert, erbt sie die Berechtigungen des Ordners, in den sie kopiert wurde. Wird eine Datei auf demselben Volume verschoben, behält sie ihre Berechtigungen. Wenn eine Datei auf ein anderes Volume verschoben wird, erbt sie die Berechtigungen des Ordners, in den sie verschoben wurde.
- Wenn Sie erstmals eine Datei verschlüsseln, erstellt Windows 7 ein EFS-Zertifikat und einen passenden privaten Schlüssel. Für ein anderes Konto können Sie eine Datei nur verschlüsseln, wenn für dieses Konto ein EFS-Zertifikat vorliegt.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 2, »Ordner- und Dateizugriff«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie sind auf einem Computer angemeldet, auf dem Windows 7 Enterprise verwendet wird und den Sie sich mit Jeff Phillips teilen. Sie möchten einige Dateien auf einem mit NTFS formatierten USB-Flashlaufwerk speichern, auf das Sie und Jeff Zugriff haben. Sie möchten diese Dateien verschlüsseln, aber nicht BitLocker To Go verwenden. Sie können diese Dateien zwar verschlüsseln, aber als Sie Jeff hinzufügen wollten,

wurde sein Zertifikat nicht angezeigt. Was müssen Sie tun, damit EFS Dateien für Ihr Konto und für Jeffs Konto verschlüsselt?

A. Sie fordern Jeff auf, sein Kennwort zu ändern.
B. Sie bringen Jeff dazu, auf dem Computer eine Datei zu verschlüsseln.
C. Sie geben Jeff die Berechtigung *Schreiben* für die Dateien.
D. Sie bringen Jeff dazu, die Dateien in Besitz zu nehmen.

2. Welche der folgenden Berechtigungen werden ebenfalls festgelegt, wenn Sie die NTFS-Berechtigung *Lesen, Ausführen (Verweigern)* einstellen? (Wählen Sie alle zutreffenden Antworten.)

A. *Ordnerinhalt anzeigen (Verweigern)*
B. *Lesen (Verweigern)*
C. *Ändern (Verweigern)*
D. *Schreiben (Verweigern)*

3. Das Benutzerkonto *Jeff_Phillips* ist Mitglied von vier separaten Sicherheitsgruppen, die alle über unterschiedliche Berechtigungen für einen Ordner auf einem Windows 7-Computer verfügen. Mit welchem der folgenden Tools können Sie herausfinden, über welche Berechtigungen für eine Datei aus diesem Ordner Jeff verfügt?

A. Robocopy
B. Icacls
C. Cipher
D. Registerkarte *Effektive Berechtigungen*

4. Der Inhalt des Ordners *C:\Quelle* wird mit EFS verschlüsselt. Der Ordner *D:\Ziel* ist komprimiert. Die Volumes C und D sind beide NTFS-Volumes. Was geschieht, wenn Sie eine Datei namens *Beispiel.txt* mit dem Windows-Explorer von *C:\Quelle* nach *D:\Ziel* verschieben? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)

A. *Beispiel.txt* bleibt verschlüsselt
B. *Beispiel.txt* wird komprimiert
C. *Beispiel.txt* behält die ursprünglichen NTFS-Berechtigungen
D. *Beispiel.txt* erbt die NTFS-Berechtigungen des Ordners *D:\Ziel*

5. Sie möchten Aufzeichnungen darüber haben, welche Benutzerkonten für Zugriffe auf Dokumente aus einem sensiblen Ordner verwendet werden, der auf einem Computer mit dem Betriebssystem Windows 7 Enterprise liegt. Was sollten Sie tun, um dieses Ziel zu erreichen?

A. Sie konfigurieren EFS
B. Sie konfigurieren die Überwachung
C. Sie konfigurieren NTFS-Berechtigungen
D. Sie konfigurieren BranchCache

Lektion 3: Verwalten von BranchCache

BranchCache ist eine neue Technologie von Windows 7 und Windows Server 2008 R2, die in Zweigstellen und Filialen den Zugriff auf Dateien und Websites von Remoteservern beschleunigen kann, die nur über WAN-Verbindungen zugänglich sind. BranchCache speichert Inhalte von den Remoteservern im LAN (Local Area Network) zwischen. Statt Inhalte stets über die langsamere WAN-Verbindung abzurufen, überprüfen Clients zuerst, ob bereits eine Kopie der gewünschten Daten lokal zwischengespeichert worden ist. Ist die Kopie vorhanden und sind bestimmte Voraussetzungen erfüllt, verwendet der Client die zwischengespeicherte Kopie. Wenn die gewünschten Daten nicht vorhanden sind, werden sie über die WAN-Verbindung angefordert, lokal zwischengespeichert und dann vom Client verwendet. Der Vorteil von BranchCache besteht darin, eine mehrfache Übertragung derselben unveränderten Datei über die WAN-Verbindung zu vermeiden und einen schnellen lokalen Zugriff zu ermöglichen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren von BranchCache mit Gruppenrichtlinien
- Konfigurieren von BranchCache mit *Netsh*
- Erläutern des Unterschieds zwischen dem verteilten und dem gehosteten Cache

Veranschlagte Zeit für diese Lektion: 40 Minuten

BranchCache-Konzepte

BranchCache ist ein Feature, das in Zweigstellen oder Filialen den Zugriff auf Dateien aus Remotenetzwerken durch Zwischenspeicherung beschleunigt. Je nach verwendetem BranchCache-Modus wird der Zwischenspeicher entweder auf einem Server unter Windows Server 2008 R2 eingerichtet oder auf die Windows 7-Clients des Zweigstellennetzwerks verteilt. BranchCache ist nur unter Windows 7-Editionen Enterprise und Ultimate verfügbar. BranchCache kann nur Daten von Datei- und Webservern zwischenspeichern, die unter Windows Server 2008 R2 eingerichtet wurden. Mit BranchCache können Sie nicht den Zugriff auf Daten beschleunigen, die auf Servern unter Windows Server 2008, Windows Server 2003 oder Windows Server 2003 R2 gespeichert sind.

BranchCache wird aktiv, wenn die Roundtrip-Netzwerklatenz für einen kompatiblen Server 80 Millisekunden übersteigt. Wenn ein Windows 7-Client BranchCache verwendet, werden einige Überprüfungen durchgeführt:

- Der Client überprüft, ob der Server, auf dem die angeforderten Daten liegen, BranchCache unterstützt.
- Der Client überprüft, ob die Roundtrip-Netzwerklatenz den Schwellenwert übersteigt.
- Der Client überprüft, ob die angeforderten Daten bereits im Zweigstellennetzwerk zwischengespeichert wurden.
  - Liegen die Daten bereits im Zwischenspeicher, wird überprüft, ob sie noch auf dem neusten Stand sind und ob der Client über die Berechtigung verfügt, auf die Daten zuzugreifen.
  - Wurden die Daten noch nicht zwischengespeichert, werden sie vom Server angefordert und im Zweigstellennetzwerk zwischengespeichert.

Die Cachemodi legen fest, wie die Zwischenspeicherung in der Zweigstelle erfolgt. Für BranchCache sind zwei Modi verfügbar: »Gehosteter Cache« oder »Verteilter Cache«. Über diese Modi erfahren Sie im Verlauf dieser Lektion mehr.

Gehosteter Cache

Im Modus »Gehosteter Cache« wird ein zentraler lokaler Zwischenspeicher verwendet, der in der Zweigstelle auf einem Server unter Windows Server 2008 R2 eingerichtet wird. Gewöhnlich können Sie den Zwischenspeicher ohne nennenswerte Leistungseinbußen auch auf einem Server einrichten, den Sie für andere Funktionen verwenden, sofern als Betriebssystem Windows Server 2008 R2 verwendet wird. Wenn nämlich die Remotezugriffe über das WAN so häufig erfolgen, dass sich eine Leistungseinbuße bemerkbar macht, würden Sie die Dateien mit einer Lösung wie DFS (Distributed File System, verteiltes Dateisystem) in die Zweigstelle replizieren, statt BranchCache zu verwenden. Der gehostete Cache hat gegenüber dem verteilten Cache den Vorteil, dass es einen zentralen Cache gibt, der immer verfügbar ist. Von einem verteilten Cache fallen Teile aus, wenn die Clients, auf denen diese Teile liegen, heruntergefahren werden. Über den Modus »Verteilter Cache« erfahren Sie mehr im Verlauf dieser Lektion.

Der Modus »Gehosteter Cache« setzt in jeder Zweigstelle einen entsprechend konfigurierten Computer voraus, auf dem Windows Server 2008 R2 verwendet wird. Sie müssen jeden BranchCache-Client mit der Adresse des BranchCache-Hostservers konfigurieren.

Wenn Sie den Server für den Modus »Gehosteter Cache« einrichten, tun Sie Folgendes:

- Installieren Sie das *BranchCache*-Feature.
- Installieren Sie ein SSL-Zertifikat (Secure Sockets Layer), dessen Antragstellername auf den vollqualifizierten Domänennamen ((Fully Qualified Domain Name, FQDN) des Cacheservers lautet. Dazu müssen Sie das SSL-Zertifikat in den Zertifikatspeicher des lokalen Computers importieren, den Zertifikatfingerabdruck notieren und das Zertifikat dann mit dem Befehl `netsh http add sslcert ipport=0.0.0.0:443 certhash=<Zertifikatfingerabdruck> APPID={d673f5ee-a714-454d-8de2-492e4c1bd8f8}` binden.
- Sorgen Sie dafür, dass alle Clients der Zertifizierungsstelle vertrauen, die das SSL-Zertifikat ausgestellt hat, das auf dem zentralen Cacheserver installiert wurde.

Der Modus »Gehosteter Cache« eignet sich nicht für Organisationen, die nicht über ihre eigene Active Directory-Zertifikatdiensteinfrastruktur verfügen oder nicht die Ressourcen haben, um in jeder Zweigstelle einen Windows Server 2008 R2-Server aufzubauen.



Weitere Informationen Konfigurieren von Cacheservern

Weitere Informationen über die Konfiguration eines Servers unter Windows Server 2008 R2 als Cacheserver, einschließlich der Änderung der verwendeten Standardports, finden Sie im folgenden TechNet-Dokument: *http://technet.microsoft.com/de-de/library/dd637793(WS.10).aspx*.

Modus »Verteilter Cache«

Im Modus »Verteilter Cache« wird Peercaching verwendet, um den Zwischenspeicher der Zweigstelle auf die Windows 7-Clients des Zweigstellennetzwerks zu verteilen. Das bedeutet, dass jeder Client in diesem Modus einen Teil des Zwischenspeichers aufnimmt, aber keiner

den gesamten Zwischenspeicher. Wenn ein Windows 7-Client über das WAN eine Datei abruft, speichert er sie in seinem eigenen Zwischenspeicher. Falls ein anderer BranchCache-Client unter Windows 7 versucht, dieselbe Datei abzurufen, kann er sie direkt vom ersten Client erhalten und muss sie nicht über die WAN-Verbindung anfordern. Wenn er die Datei vom ersten Client erhält, speichert er diese Datei ebenfalls in seinem eigenen Zwischenspeicher.

Der Vorteil des Modus »Verteilter Cache« liegt darin, dass kein zusätzlicher Windows Server 2008 R2-Server in der Zweigstelle eingerichtet werden muss. Allerdings hat der Modus »Verteilter Cache« den Nachteil, dass der Inhalt eines Zwischenspeichers aus dem Zweigstellennetzwerk davon abhängt, welche Clients online sind. Braucht ein Client eine Datei, die sich im Zwischenspeicher eines heruntergefahrenen Computers befindet, muss er die Datei über das WAN vom Hostserver anfordern.

Schnelltest

- Welchen BranchCache-Modus sollten Sie verwenden, wenn in Ihrer Zweigstelle keine Server verfügbar sind, auf denen Windows Server 2008 R2 ausgeführt wird?

Antwort zum Schnelltest

- Sie sollten den Modus »Verteilter Cache« verwenden. Der Modus »Gehosteter Cache« setzt im LAN die Verfügbarkeit eines Servers voraus, auf dem Windows Server 2008 R2 ausgeführt wird.

Konfigurieren der Windows 7-BranchCache-Clients

Um Windows 7 als BranchCache-Client zu konfigurieren, müssen Sie BranchCache aktivieren, sei es im Modus »Gehosteter Cache« oder im Modus »Verteilter Cache«, und dann die Clientfirewall konfigurieren, damit sie den BranchCache-Datenverkehr zulässt. BranchCache lässt sich mit Gruppenrichtlinien oder mit dem Befehlszeilenprogramm Netsh konfigurieren. Welche Firewallregeln erforderlich sind, hängt davon ab, ob Sie den Modus »Hosted Cache« oder »Verteilter Cache« verwenden. Sie können vordefinierte Firewallregeln verwenden oder die Regeln auf der Basis von Protokoll und Port erstellen. Folgende Firewallregeln sind erforderlich:

- **Die vordefinierte Regel *BranchCache – Inhaltsabruf (verwendet HTTP)*** Wenn diese Regel nicht verfügbar ist, erstellen Sie Regeln, die eingehenden und ausgehenden Datenverkehr auf TCP-Port 80 zulassen. Diese Regel ist für beide Modi, »Hosted Cache« und »Verteilter Cache«, erforderlich. Sie können diese Regel mit der Windows-Firewall mit erweiterter Sicherheit erstellen (Abbildung 8.35).
- **Die vordefinierte Regel *BranchCache – Peerermittlung (verwendet WSD)*** Wenn diese Regel nicht verfügbar ist, erstellen Sie Regeln, die eingehenden und ausgehenden Datenverkehr auf UDP-Port 3702 zulassen. Diese Regel ist nur bei Verwendung des Modus »Verteilter Cache« erforderlich.
- **Die vordefinierte Regel *BranchCache – Gehosteter Cacheclient (verwendet HTTPS)*** Wenn diese Regel nicht verfügbar ist, konfigurieren Sie eine Regel, die ausgehenden Datenverkehr auf TCP-Port 443 zulässt. Diese Regel ist nur für den Modus »Gehosteter Cache« erforderlich.

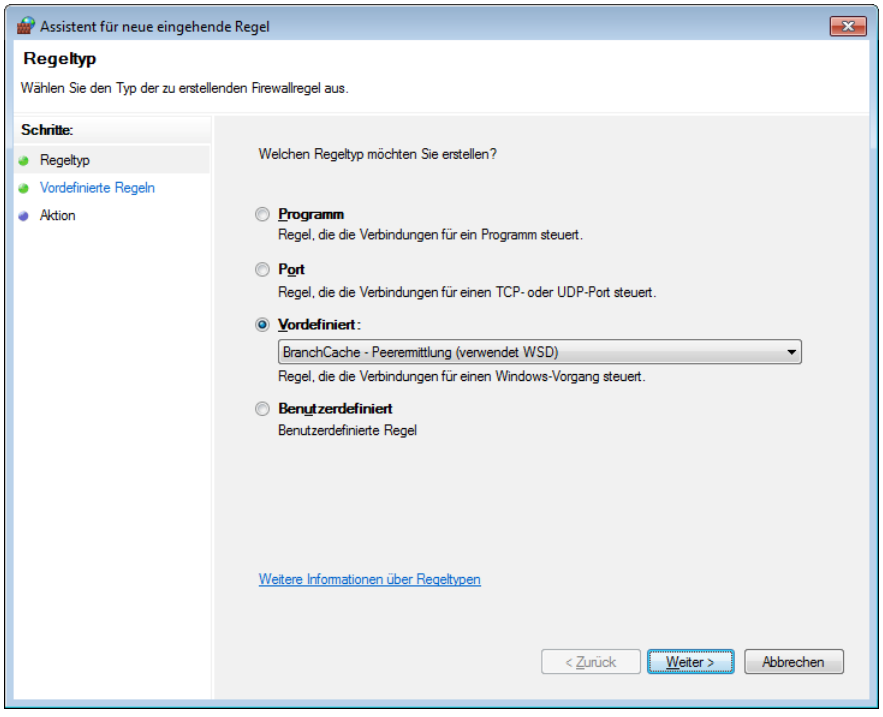


Abbildung 8.35 Vordefinierte BranchCache-Firewallregel

Sie brauchen die Firewallregeln nur zu konfigurieren, wenn Sie BranchCache mit Gruppenrichtlinien konfigurieren. Wenn Sie BranchCache mit Netsh konfigurieren, werden die erforderlichen Firewallregeln automatisch eingerichtet (Abbildung 8.36).

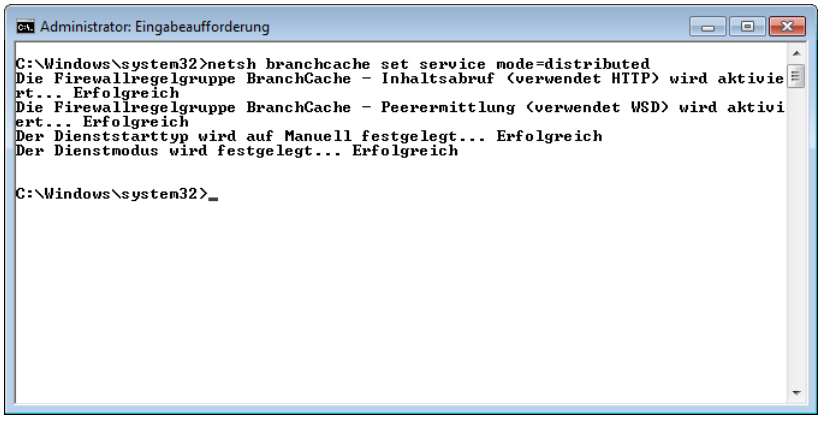

Administrator: Eingabeaufforderung
C:\Windows\system32>netsh branchcache set service mode=distributed
Die Firewallregelgruppe BranchCache - Inhaltsabruf (verwendet HTTP) wird aktivie
rt... Erfolgreich
Die Firewallregelgruppe BranchCache - Peerermittlung (verwendet WSD) wird aktivi
ert... Erfolgreich
Der Dienststarttyp wird auf Manuell festgelegt... Erfolgreich
Der Dienstmodus wird festgelegt... Erfolgreich
C:\Windows\system32>

Abbildung 8.36 Firewallregeln werden automatisch konfiguriert

Konfigurieren von BranchCache mit Gruppenrichtlinien

BranchCache kann mit Netsh oder mit Gruppenrichtlinien konfiguriert werden. Wahrscheinlich werden Sie Gruppenrichtlinien verwenden, wenn Sie auf einer großen Zahl von Computern dieselben Einstellungen vornehmen möchten. Wenn Sie BranchCache auf Windows 7-

Clients mit Gruppenrichtlinien konfigurieren möchten, öffnen Sie den Editor für lokale Gruppenrichtlinien und navigieren zum Knoten *Computerkonfiguration\Administrative Vorlagen\Netzwerk\BranchCache*. Wie Abbildung 8.37 zeigt, gibt es fünf Richtlinien für BranchCache.

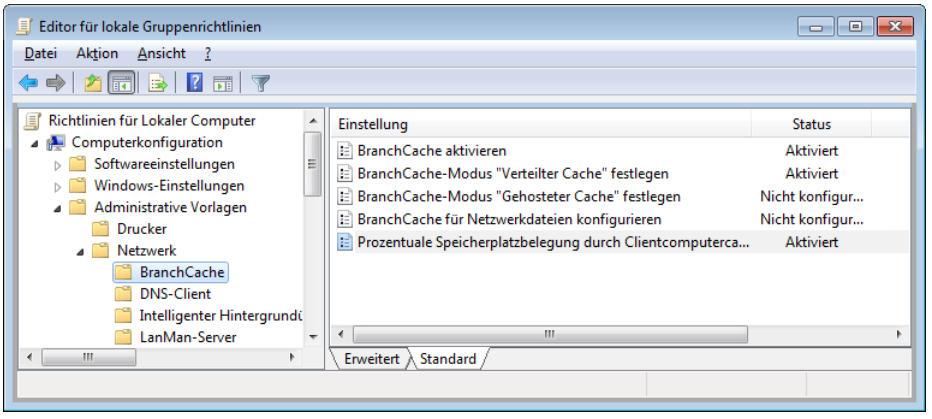


Abbildung 8.37 BranchCache-Richtlinien

Diese Richtlinien haben folgende Aufgaben:

- **BranchCache aktivieren** Diese Richtlinie aktiviert BranchCache und konfiguriert den *BranchCache*-Dienst für den automatischen Start. Windows startet den Dienst, wenn Sie versuchen, Daten von einem kompatiblen Remoteserver anzufordern, und die Roundtrip-Netzwerklatenz den Schwellenwert überschreitet.
- **BranchCache-Modus "Verteilter Cache" festlegen** Diese Richtlinie stellt für den Client den Modus »Verteilter Cache« ein. Damit diese Richtlinie wirken kann, aktivieren Sie außerdem die Richtlinie *BranchCache aktivieren*.
- **BranchCache-Modus "Gehosteter Cache" festlegen** Diese Richtlinie stellt für den Client den Modus »Gehosteter Cache« ein. Wenn Sie diese Richtlinie aktivieren, müssen Sie den vollständigen Domänennamen des Hostcacheservers angeben (Abbildung 8.38). Das auf dem Server installierte SSL-Zertifikat muss zu diesem vollständigen Domänennamen passen und der Client muss der ausstellenden Zertifizierungsstelle vertrauen. Damit diese Richtlinie wirken kann, aktivieren Sie außerdem die Richtlinie *BranchCache aktivieren*.
- **BranchCache für Netzwerkdateien konfigurieren** Diese Richtlinie ermöglicht Ihnen die Festlegung des Schwellenwerts für die Roundtrip-Netzwerklatenz, bei dessen Überschreitung BranchCache verwendet wird. Wenn Sie diese Richtlinie nicht konfigurieren, wird der Standardwert 80 Millisekunden verwendet. Sie brauchen diese Richtlinie nur zu konfigurieren, wenn der Standardwert von 80 Millisekunden für die Netzwerkumgebung Ihrer Organisation ungeeignet ist.
- **Prozentuale Speicherplatzbelegung durch Clientcomputercache festlegen** Mit dieser Richtlinie können Sie festlegen, welcher prozentuale Anteil des Gesamtspeicherplatzes der Festplatte für die Speicherung von BranchCache-Dateien verwendet werden soll. Andere Clients aus dem Zweigstellennetzwerk können auf diese Dateien zugreifen, wenn der Modus »Verteilter Cache« verwendet wird. Wenn Sie diese Richt-

linie nicht aktivieren, werden 5 Prozent des gesamten Festplattenspeicherplatzes des Computers für den Zwischenspeicher verwendet.

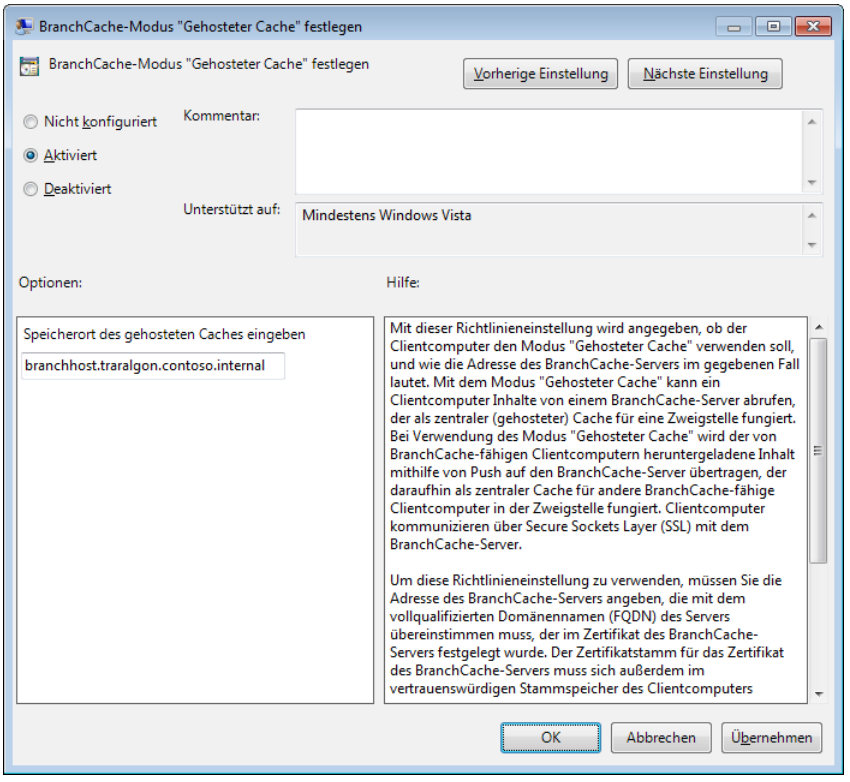

BranchCache-Modus "Gehosteter Cache" festlegen
BranchCache-Modus "Gehosteter Cache" festlegen
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows Vista
Optionen:
Hilfe:
Speicherort des gehosteten Caches eingeben
branchhost.traralgon.contoso.internal
Mit dieser Richtlinieneinstellung wird angegeben, ob der Clientcomputer den Modus "Gehosteter Cache" verwenden soll, und wie die Adresse des BranchCache-Servers im gegebenen Fall lautet. Mit dem Modus "Gehosteter Cache" kann ein Clientcomputer Inhalte von einem BranchCache-Server abrufen, der als zentraler (gehosteter) Cache für eine Zweigstelle fungiert. Bei Verwendung des Modus "Gehosteter Cache" wird der von BranchCache-fähigen Clientcomputern heruntergeladene Inhalt mithilfe von Push auf den BranchCache-Server übertragen, der daraufhin als zentraler Cache für andere BranchCache-fähige Clientcomputer in der Zweigstelle fungiert. Clientcomputer kommunizieren über Secure Sockets Layer (SSL) mit dem BranchCache-Server.
Um diese Richtlinieneinstellung zu verwenden, müssen Sie die Adresse des BranchCache-Servers angeben, die mit dem vollqualifizierten Domänennamen (FQDN) des Servers übereinstimmen muss, der im Zertifikat des BranchCache-Servers festgelegt wurde. Der Zertifikatstamm für das Zertifikat des BranchCache-Servers muss sich außerdem im vertrauenswürdigen Stammspeicher des Clientcomputers
OK
Abbrechen
Übernehmen

Abbildung 8.38 Die Richtlinie *BranchCache-Modus "Gehosteter Cache" festlegen*

Konfigurieren von BranchCache mit Netsh

Sie können Netsh im Kontext *BranchCache* verwenden, um BranchCache zu konfigurieren und Probleme mit BranchCache zu beheben. Es gibt einige Netsh-Optionen, beispielsweise die lokale Zwischenspeicherung, die bei der Konfiguration von BranchCache mit Gruppenrichtlinien nicht zur Verfügung stehen. Ein weiterer Vorteil von Netsh besteht darin, dass die erforderlichen Firewallregeln für die BranchCache-Modi automatisch aktiviert werden. Wenn Sie BranchCache mit Gruppenrichtlinien aktivieren, müssen Sie auch die entsprechenden Firewallregeln konfigurieren. Diese Firewallregeln haben Sie in dieser Lektion bereits kennen gelernt.

Bis auf `show status` müssen alle `netsh branchcache`-Befehle in einer Eingabeaufforderung mit erhöhten Rechten verwendet werden. Zur Konfiguration von BranchCache können Sie folgende Befehle verwenden:

- **Netsh BranchCache reset** Dieser Befehl setzt die aktuelle BranchCache-Konfiguration zurück, deaktiviert und beendet den Dienst, stellt die Standardwerte in der Registrierung wieder her, löscht alle Zwischenspeicherdateien und stellt den Starttyp des Dienstes auf *Manuell*. Dieser Befehl deaktiviert auch die konfigurierten BranchCache-Firewallregeln.

- **Netsh BranchCache show status** Dieser Befehl zeigt den aktuellen Dienstmodus und den aktuellen Status des *BranchCache*-Dienstes an. Aus den Angaben geht auch hervor, ob der Dienstmodus mit Gruppenrichtlinien konfiguriert wurde.
- **netsh branchcache set service mode=distributed** Dieser Befehl stellt den Modus »Verteilter Cache« ein, startet den *BranchCache*-Dienst und ändert den Starttyp auf *Manuell*. Außerdem aktiviert er die Firewallregeln *BranchCache – Inhaltsabruf (verwendet HTTP)* und *BranchCache – Peerermittlung (verwendet WSD)*.
- **netsh branchcache set service mode=local** Dieser Befehl stellt die lokale Zwischenspeicherung ein, startet den *BranchCache*-Dienst und ändert den Starttyp auf *Manuell*. Er aktiviert keine Firewallregeln. Wenn Sie die lokale Zwischenspeicherung einstellen, speichert der Client die aus dem WAN angeforderten Dateien zwar in einem lokalen Zwischenspeicher, gibt den Inhalt dieses Zwischenspeichers aber nicht für andere Clients aus dem Zweigstellennetzwerk frei. Dieser Modus lässt sich nur mit Netsh einstellen.
- **netsh branchcache set service mode=hostedclient location=<*Cacheserver*>** Dieser Befehl stellt den Modus »Gehosteter Cache« ein, legt den Cacheserver fest, startet den *BranchCache*-Dienst und ändert den Starttyp auf *Manuell*. Außerdem aktiviert er die Firewallregeln *BranchCache – Inhaltsabruf (verwendet HTTP)* und *BranchCache – Gehosteter Cacheclient (verwendet HTTPS)*.
- **Netsh BranchCache set cachesize** Mit dieser Richtlinie können Sie die Größe des lokalen Zwischenspeichers festlegen. Geben Sie die Größe prozentual oder in Byte an.
- **Netsh BranchCache set localcache** Mit dieser Richtlinie können Sie den Speicherort des lokalen Zwischenspeichers festlegen.

Konfigurationseinstellungen, die mit Gruppenrichtlinien vorgenommen werden, haben Vorrang vor den Einstellungen, die mit Netsh erfolgen.

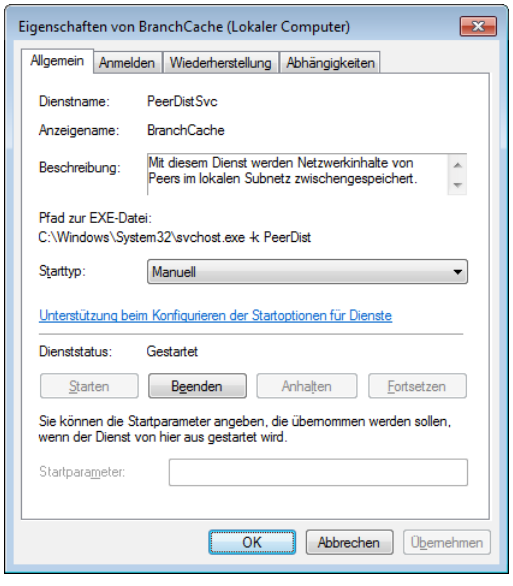


Abbildung 8.39 Der Status des *BranchCache*-Dienstes

Überprüfen des Status des *BranchCache*-Dienstes

Mit der Konsole *Dienste* können Sie den Status des *BranchCache*-Dienstes überprüfen, der gestartet sein muss, damit BranchCache funktioniert. Um diese Konsole zu öffnen, können Sie im Textfeld *Programme/Dateien durchsuchen* des *Start*-Menüs **services.msc** eingeben. Zur Öffnung des Eigenschaftendialogfelds des Dienstes klicken Sie den Dienst *BranchCache* mit einem Doppelklick an. Überprüfen Sie, ob der Dienst gestartet und der Starttyp *Manuell* eingestellt wurde (Abbildung 8.39).

Konfigurieren von Datei- und Webservern unter Windows Server 2008 R2

BranchCache funktioniert nur, wenn Daten von Web- und Dateiservern abgerufen werden, die unter Windows Server 2008 R2 betrieben werden. So konfigurieren Sie einen Server für BranchCache:

1. Installieren Sie mit dem Assistenten zum Hinzufügen von Features auf dem Windows Server 2008 R2-Server das Feature *BranchCache* (Abbildung 8.40). Die Rolle *Webserver* von Windows Server 2008 R2 verwendet automatisch BranchCache, nachdem Sie das Feature *BranchCache* installiert haben.

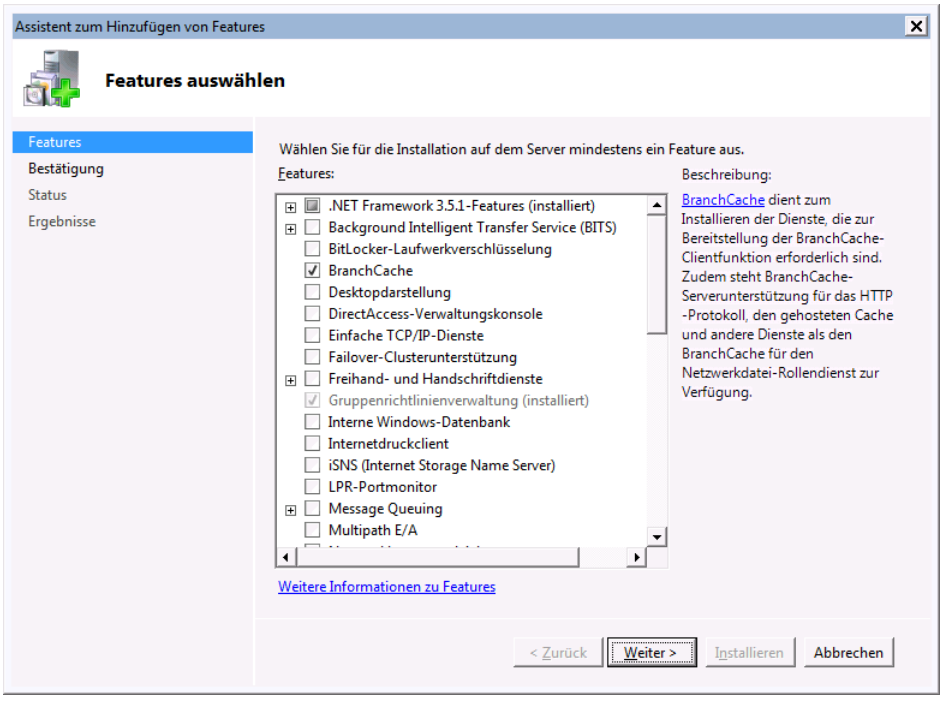


Abbildung 8.40 Installieren des Features *BranchCache* unter Windows Server 2008 R2

2. Sorgen Sie dafür, dass Sie den Rollendienst *BranchCache für Netzwerkdateien* hinzufügen, wenn Sie die Rolle *Dateidienste* installieren (Abbildung 8.41).

3. Bearbeiten Sie die Richtlinie *Computerkonfiguration\Richtlinie\Administrative Vorlagen\Netzwerk\LanMan-Server\Hashveröffentlichung für BranchCache*. Aktivieren Sie die Richtlinie und wählen Sie eine der folgenden Optionen:
   - *Hashveröffentlichung nur für freigegebene Ordner mit aktiviertem BranchCache zulassen*
   - *Hashveröffentlichung für alle freigegebenen Ordner zulassen*

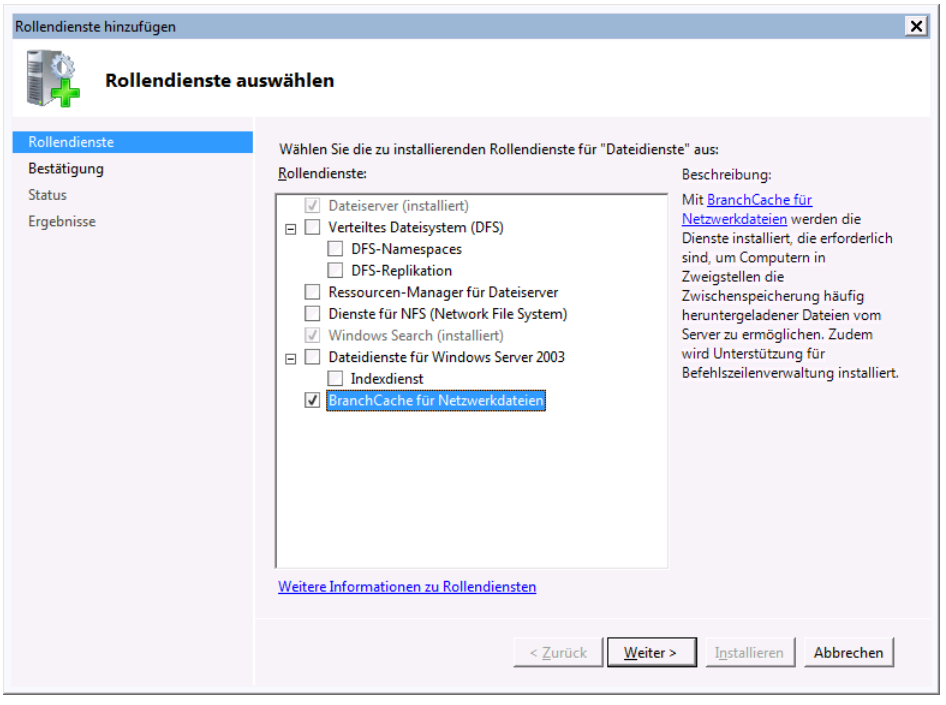


Abbildung 8.41 Installieren von BranchCache für Netzwerkdateien

4. Wenn Sie BranchCache nur für ausgewählte freigegebene Ordner aktivieren möchten, öffnen Sie unter Windows Server 2008 R2 der Reihe nach in der Konsole *Freigabe- und Speicherverwaltung* das Eigenschaftendialogfeld jeder Freigabe, die Sie mit BranchCache verwenden wollen, und klicken dann auf *Erweitert*. Aktivieren Sie BranchCache im Dialogfeld *Erweitert* (Abbildung 8.42).

Weitere Informationen **Konfigurieren von Servern für BranchCache**

Weitere Informationen über die Konfiguration von Windows Server 2008 R2 für BranchCache erhalten Sie in folgendem TechNet-Dokument: *http://technet.microsoft.com/de-de/library/dd637785(WS.10).aspx*.

Prüfungstipp

Merken Sie sich die Syntax des Befehls `netsh branchcache set service` und dass er den BranchCache-Dienst und die Firewallregeln automatisch konfiguriert.

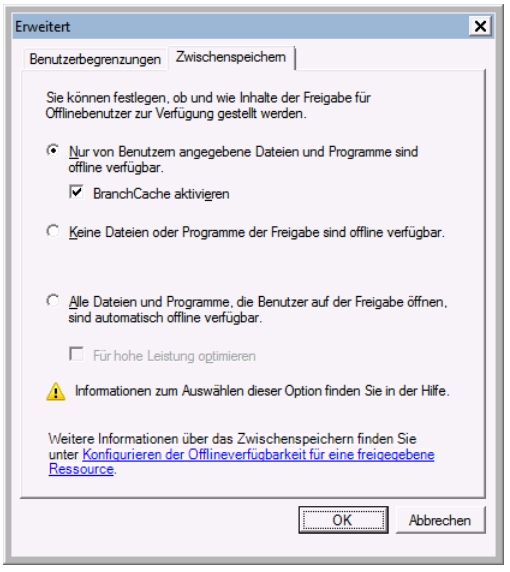

Erweitert
Benutzerbegrenzungen
Zwischenspeichern
Sie können festlegen, ob und wie Inhalte der Freigabe für Offlinebenutzer zur Verfügung gestellt werden.
Nur von Benutzern angegebene Dateien und Programme sind offline verfügbar.
BranchCache aktivieren
Keine Dateien oder Programme der Freigabe sind offline verfügbar.
Alle Dateien und Programme, die Benutzer auf der Freigabe öffnen, sind automatisch offline verfügbar.
Für hohe Leistung optimieren
Informationen zum Auswählen dieser Option finden Sie in der Hilfe.
Weitere Informationen über das Zwischenspeichern finden Sie unter Konfigurieren der Offlineverfügbarkeit für eine freigegebene Ressource.
OK
Abbrechen

Abbildung 8.42 Aktivieren von BranchCache für eine Freigabe

Übung BranchCache-Konfiguration

BranchCache kann in einer Zweigstelle oder Filiale auf den Windows 7-Clients des Netzwerks einen verteilten Zwischenspeicher für Remotedateien und Webserverdaten einrichten. Der verteilte Zwischenspeicher kann in den Gruppenrichtlinien oder mit dem Befehlszeilenprogramm Netsh konfiguriert werden.

Übung Konfigurieren von BranchCache

In dieser Übung konfigurieren Sie die BranchCache-Clienteinstellungen auf einem Windows 7-Computer mit dem Befehlszeilenprogramm Netsh:

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
3. Verwenden Sie folgenden Befehl:

   ```
   Netsh BranchCache show status
   ```

4. Überprüfen Sie, ob der Dienstmodus auf *Deaktiviert* eingestellt und der aktuelle Status des Dienstes *Beendet* ist.
5. Verwenden Sie folgenden Befehl:

   ```
   netsh branchcache set service mode=distributed
   ```

6. Überprüfen Sie, ob die Statusmeldungen die Aktivierung von zwei Firewallregeln bestätigen und der Dienststarttyp auf *Manuell* eingestellt ist.
7. Verwenden Sie folgenden Befehl:

   ```
   Netsh BranchCache show status
   ```

8. Überprüfen Sie, ob der Dienstmodus auf *Distributed Caching* eingestellt ist und der aktuelle Dienststatus *Wird ausgeführt* angezeigt wird.

9. Verwenden Sie folgenden Befehl:

   ```
   Netsh BranchCache set cachesize size=25 percent=True
   ```

10. Verwenden Sie folgenden Befehl:

    ```
    Netsh BranchCache show localcache
    ```

11. Überprüfen Sie, ob die maximale Größe des Zwischenspeichers auf 25 Prozent der Festplatte eingestellt ist.
12. Verwenden Sie folgenden Befehl:

    ```
    Netsh BranchCache reset
    ```

Zusammenfassung der Lektion

- BranchCache ermöglicht die Zwischenspeicherung von Dateien, die auf Remotedateiservern unter Windows Server 2008 R2 gespeichert sind, im Netzwerk einer Zweigstelle.
- Nur die Editionen Windows 7 Enterprise und Ultimate unterstützen BranchCache.
- Im Modus »Verteilter Cache« wird der Zwischenspeicher auf die Windows 7-Clients aufgeteilt.
- Der Modus »Gehosteter Cache« erfordert einen speziell konfigurierten Server, auf dem Windows Server 2008 R2 ausgeführt wird.
- Wenn Sie mit Netsh den Modus »Verteilter Cache« oder »Gehosteter Cache« aktivieren, werden der *BranchCache*-Dienst und die Firewallregeln automatisch konfiguriert.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 3, »Verwalten von BranchCache«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie möchten in den Zweigstellen Ihrer Organisation BranchCache im Modus »Gehosteter Cache« verwenden. In der Zentrale Ihrer Organisation haben Sie BranchCache bereits auf den Servern aktiviert. Was müssen Sie nun tun? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)
   A. Sie stellen in jeder Zweigstelle mindestens einen Server bereit, auf dem Windows Server 2008 R2 ausgeführt wird.
   B. Sie aktualisieren alle Clientcomputer in den Zweigstellen auf Windows 7 Enterprise.
   C. Sie aktualisieren alle Clientcomputer in den Zweigstellen auf Windows 7 Professional.
   D. Sie stellen in jeder Zweigstelle mindestens einen Windows Server 2008-RODC (Read-Only Domain Controller) bereit.

2. Mit welchem der folgenden Tools können Sie eine Gruppe von Windows 7-Clients so konfigurieren, dass sie BranchCache im Peercaching-Modus verwenden? (Wählen Sie alle zutreffenden Antworten.)
   A. `net share`
   B. Netsh
   C. Ipconfig
   D. Editor für lokale Gruppenrichtlinien
3. In einer der Zweigstellen Ihrer Organisation gibt es zwei Computer, auf denen Windows 7 Ultimate verwendet wird. Auf allen Servern dieser Zweigstelle wird Windows Server 2003 R2 verwendet. Sie möchten einen dieser Computer so konfigurieren, dass er Dateien zwischenspeichert, die von einem Dateiserver aus der Zentrale angefordert werden. Auf diesem Dateiserver mit dem Namen *fs-alpha.contoso.internal* wird Windows Server 2008 R2 ausgeführt. Auf ihm werden sensible Daten gespeichert. Der Computer, den Sie konfigurieren, soll die zwischengespeicherten Dateien nicht an den anderen Windows 7 Ultimate-Computer im Netzwerk weitergeben. Welchen der folgenden Befehle sollten Sie zur Konfiguration des Computers verwenden?
   A. `netsh branchcache set service disabled`
   B. `netsh branchcache set service mode=distributed`
   C. `netsh branchcache set service mode=local`
   D. `netsh branchcache set service mode=hostedclient location=fs-alpha.contoso.internal`
4. Sie möchten Clients, auf denen Windows 7 Enterprise verwendet wird, in einer Zweigstelle für den BranchCache-Modus »Gehosteter Cache« konfigurieren. Als Host dient im LAN ein Server namens *branch-1.contoso.internal*, auf dem Windows Server 2008 R2 verwendet wird. Welchen der folgenden Befehle sollten Sie zur Konfiguration der Windows 7-Clients verwenden (in einer Eingabeaufforderung mit erhöhten Rechten)?
   A. `netsh branchcache set service mode=distributed`
   B. `netsh branchcache set service mode=local`
   C. `netsh branchcache set service mode=hostedserver clientauthentication=domain`
   D. `netsh branchcache set service mode=hostedclient location=branch-1.contoso.internal`
5. Sie möchten die Clients einer Zweigstelle so konfigurieren, dass BranchCache nur verwendet wird, wenn die Roundtrip-Netzwerklatenz beim Zugriff über das WAN größer ist als 120 Millisekunden. Mit welcher der folgenden Richtlinien erreichen Sie dieses Ziel?
   A. *BranchCache für Netzwerkdateien konfigurieren*
   B. *Prozentuale Speicherplatzbelegung durch Clientcomputercache festlegen*
   C. *BranchCache-Modus "Verteilter Cache" festlegen*
   D. *BranchCache-Modus "Gehosteter Cache" festlegen*

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Heimnetzgruppen ermöglichen die gemeinsame Verwendung von Ressourcen im Heimnetzwerk.
- Mit der Konsole *Computerverwaltung* können Sie freigegebene Ordner zentral verwalten.
- Bibliotheken sind Sammlungen von Ordnern mit ähnlichen Inhalten.
- NTFS-Berechtigungen legen fest, auf welche Dateien ein Benutzer oder eine Gruppe zugreifen kann.
- Druckerberechtigungen legen die Berechtigungen eines Benutzers zur Verwaltung von Druckern und Dokumenten fest.
- BranchCache ist eine Technologie zur Beschleunigung des Dateizugriffs in Zweigstellen und Filialen durch Zwischenspeicherung bereits verwendeter Dateien im Zweigstellennetzwerk.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **BranchCache**
- **Verschlüsselndes Dateisystem (EFS)**
- **Heimnetzgruppe**
- **Bibliothek**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie Ihr Wissen zum Stoff dieses Kapitels an. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: Berechtigungen und Verschlüsselung

Ein Computer namens Waverley, auf dem Windows 7 Enterprise ausgeführt wird, verfügt über die beiden mit NTFS formatierten Volumes *C* und *D*. Der Ordner *C:\Freigabe* wurde freigegeben und enthält 15 Unterordner und Hunderte von Dateien. Für viele dieser Ordner wurden spezielle NTFS-Berechtigungen festgelegt. Sie möchten den Ordner nun auf Volume *D* verschieben, weil auf Volume *C* zu wenig Platz ist. Einer der Benutzer wechselt vom Computer Waverley auf den Computer Warrandyte. Dieser Benutzer hat eine große Zahl von EFS-verschlüsselten Dateien auf ein mit NTFS formatiertes USB-Flashlaufwerk kopiert.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Was tun Sie, damit der Benutzer auf dem Computer Warrandyte die verschlüsselten Dateien auf dem USB-Flashlaufwerk lesen kann?
2. Was können Sie tun, damit alle Dateien wiederhergestellt werden können, die zukünftig verschlüsselt werden?
3. Wie verschieben Sie den freigegebenen Ordner auf Volume *D*?

Übung 2: Konfigurieren der Contoso-Zweigstellen

Sie versuchen, die verfügbare WAN-Übertragungskapazität zwischen der Contoso-Zentrale in Melbourne und den Zweigstellen in Wangaratta und Traralgon effizienter zu nutzen. Auf allen Clientcomputern von Contoso ist Windows 7 Enterprise installiert. Im Verlauf des Arbeitstages schalten die Benutzer ihre Computer ein und wieder aus. Wenn es möglich ist, wollen Sie BranchCache-Daten aber so speichern, dass sie möglichst immer verfügbar sind. Am Standort Traralgon gibt es einen Windows Server 2008 R2-RODC namens *rodc.traralgon.contoso.internal* und am Standort Wangaratta gibt es einen Windows Server 2008-RODC namens *rodc.wangaratta.contoso.internal*. Es gibt keine Pläne, in der näheren Zukunft Serverbetriebssysteme zu aktualisieren.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Welchen BranchCache-Modus sollten Sie in der Zweigstelle Wangaratta verwenden?
2. Welchen BranchCache-Modus sollten Sie in der Zweigstelle Traralgon verwenden?
3. Was müssen Sie tun, um den Server *rodc.traralgon.contoso.internal* auf BranchCache vorzubereiten?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Konfigurieren von freigegebenen Ressourcen

Führen Sie diese Übung durch, wenn Sie mit dem Benutzerkonto *Kim_Akers* am Computer *Canberra* angemeldet sind.

- Konfigurieren Sie einen freigegebenen Drucker. Erstellen Sie eine lokale Gruppe namens *PrinterManagers* und weisen Sie dieser Gruppe die Berechtigung zum Verwalten des Druckers zu.

Konfigurieren des Datei- und Ordnerzugangs

Führen Sie diese Übungen durch, wenn Sie mit dem Benutzerkonto *Kim_Akers* am Computer *Canberra* angemeldet sind.

- **Übung 1** Verwenden Sie *Gpedit.msc* und *Cipher.exe*, um ein EFS-Wiederherstellungsagentzertifikat zu erstellen und zu konfigurieren.
- **Übung 2** Erstellen Sie eine Datei namens *Gamma.txt*. Verwenden Sie *Icacls.exe*, um die Berechtigung *Ändern (Verweigern)* für diese Datei zuzuweisen. Kopieren Sie *Gamma.txt* mit *RoboCopy.exe* in einen neuen Ordner und überprüfen Sie, ob die Berechtigungen erhalten geblieben sind.

Konfigurieren von BranchCache

Führen Sie diese Übung durch, wenn Sie mit dem Benutzerkonto *Kim_Akers* am Computer *Canberra* angemeldet sind.

- Konfigurieren Sie den Computer *Canberra* mit dem Befehl Netsh so, dass nur eine lokale Zwischenspeicherung erfolgt.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

KAPITEL 9

Authentifizierung und Benutzerkontensteuerung

Die Benutzerkontensteuerung (User Account Control, UAC) ist ein Hilfsmittel für Administratoren, das darauf hinweist, wenn ein Vorgang ausgeführt werden soll, für den Administratorrechte erforderlich sind. Sie sollten nicht überrascht sein, wenn bei der Änderung von Firewallregeln eine Bestätigungsaufforderung der Benutzerkontensteuerung erscheint. Allerdings sollten Sie sehr misstrauisch werden, wenn sich die Benutzerkontensteuerung meldet, nur weil Sie ein Bild öffnen, das Ihnen Ihre Tante geschickt hat und das eine Katze zeigt, die einen Cheeseburger isst. Für die eine Arbeit sind Administratorrechte erforderlich, für die andere nicht. Die Benutzerkontensteuerung kann Ihren Computer vor Malware bewahren, weil Sie jedes Mal darauf hingewiesen werden, wenn ein Programm oder Dokument Administratorrechte anfordert, das diese Rechte nicht braucht. Normale Benutzer sind von der Benutzerkontensteuerung kaum betroffen, weil normale Benutzer per Definition nichts tun, für das Administratorrechte erforderlich sind. Im ersten Teil des Kapitels erfahren Sie, wie Sie die Benutzerkontensteuerung für Ihre Umgebungen konfigurieren können, damit die Benutzerkontensteuerung Sie warnt, wenn es wichtig ist, aber sonst nicht stört.

Kennwörter sind der wichtigste Schutz, wenn es um die Absicherung eines Windows 7-Computers geht. Die Sicherheit eines Kennworts entspricht der Sicherheit, die es bietet. Wenn Kennwörter für Ihre Umgebung nicht sicher genug sind, können Sie Windows 7 so konfigurieren, dass sich Benutzer nur mit einer Smartcard anmelden können. Berechtigungen und Rechte ermöglichen es Benutzern, Arbeiten durchzuführen. Sie können einem Benutzer Rechte zuweisen, beispielsweise das Recht, eine Datensicherung des gesamten Computers durchzuführen, indem Sie ihn zur entsprechenden Gruppe hinzufügen oder die erforderlichen Einstellungen in den Gruppenrichtlinien vornehmen. Im zweiten Teil des Kapitels erfahren Sie, wie Kennwortrichtlinien konfiguriert, Authentifizierungsprobleme behoben und Rechte zugewiesen werden. Außerdem wird die Sicherung und Wiederherstellung von gespeicherten Anmeldeinformationen besprochen.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren der Benutzerkontensteuerung
- Konfigurieren der Authentifizierung und Autorisierung

Lektionen in diesem Kapitel:

- Lektion 1: Verwalten der Benutzerkontensteuerung 477
- Lektion 2: Windows 7-Authentifizierung und -autorisierung 493

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels ist folgende Vorbereitung erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Client-PC namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.

Praxistipp

Orin Thomas

Die Benutzerkontensteuerung meldet sich nicht willkürlich. Sie informiert Sie, wenn Software etwas Verdächtiges tut. Wenn Sie im Inneren des Betriebssystems herumwühlen, werden Sie eine Reihe von Meldungen der Benutzerkontensteuerung erhalten, denn zur Durchführung von Änderungen am Betriebssystem brauchen Sie Administratorrechte. Wenn Sie aber etwas völlig Normales mit dem Computer machen und zum Beispiel ein Spiel spielen oder mit einem Textverarbeitungsprogramm arbeiten (für beides sollten keine Administratorrechte erforderlich sein), und die Benutzerkontensteuerung meldet sich, sollten Sie sich nicht über die aufdringliche Benutzerkontensteuerung ärgern, sondern eher nachprüfen, warum sich die Benutzerkontensteuerung meldet. Normale Programme brauchen keine Administratorrechte, um ausgeführt zu werden. Das ist einer der Schlüsselaspekte der Benutzerkontensteuerung. Wenn die Benutzerkontensteuerung Sie stört, während Sie etwas tun, was nichts mit der Computerkonfiguration zu tun hat, sollten Sie misstrauisch werden. Betrachten Sie die Benutzerkontensteuerung als rote Flagge, die Sie auf etwas hinweist, das Sie näher untersuchen sollten.

Die Benutzerkontensteuerung ist die Art des Benutzers, Sie zu fragen: »Bist Du sicher, dass dieses Programm Administratorrechte erhalten soll?« Die Antwort auf diese Frage ist wichtig. Um die Kontrolle über Ihren Computer zu erhalten, muss Malware die eigenen Berechtigungen anheben, damit sie mit Administratorrechten laufen kann. Malware-Autoren kennen sehr viele Tricks, mit denen sie versuchen, Benutzer dazu zu bringen, ihre Programme zu starten. Manchmal versucht Malware, huckepack auf anderen Programmen ans Ziel zu kommen, die Sie regelmäßig verwenden. Sie starten das Programm, halten es für etwas anderes, und schon ist es passiert! Die Benutzerkontensteuerung kann Sie nicht davon abhalten, die Malware zu starten, aber sie kann Sie darauf hinweisen, wenn das Programm etwas tut, für das Administratorrechte erforderlich sind. Wenn dies in einer Situation geschieht, in der Sie etwas tun, für das eigentlich keine Administratorrechte erforderlich sind, stellt es Ihnen die Benutzerkontensteuerung frei, damit fortzufahren. Falls Ihr Computer auf diese Weise mit Malware infiziert wird, können Sie allerdings nicht mehr sagen, niemand hätte Sie gewarnt.

Lektion 1: Verwalten der Benutzerkontensteuerung

Die Benutzerkontensteuerung (User Account Control, UAC) ist ein Tool, das Sie wahrscheinlich nur verwenden, wenn Sie sich mit einem Konto anmelden, das zur lokalen Gruppe *Administratoren* gehört. Für Standardbenutzer ist die Benutzerkontensteuerung standardmäßig deaktiviert. Das bedeutet, dass ein Standardbenutzer gewöhnlich nichts mit der Benutzerkontensteuerung zu tun hat. Das Verhalten der Benutzerkontensteuerung lässt sich genauer einstellen und an die Erfordernisse Ihrer Organisation anpassen. In dieser Lektion erfahren Sie, wie Sie die Benutzerkontensteuerung so konfigurieren können, dass sie nicht auf dem sicheren Desktop ausgeführt werden muss, wie man von Administratoren die Eingabe eines Kennworts verlangt, statt nur auf *OK* zu klicken, und wie man die Benutzerkontensteuerung so konfigurieren kann, dass Administratoren, die Standardbenutzer unterstützen, erhöhte Rechte erhalten können.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren der lokalen Sicherheitsrichtlinien für die Benutzerkontensteuerung
- Konfigurieren des Verhaltens der Anhebungsaufforderung der Benutzerkontensteuerung
- Konfigurieren des Verhaltens des sicheren Desktops

Veranschlagte Zeit für diese Lektion: 40 Minuten

Benutzerkontensteuerung

Die Benutzerkontensteuerung ist eine Sicherheitsfunktion von Windows 7, die Sie darüber informiert, wenn für die Arbeit, die Sie durchführen wollen, eine Anhebung der Rechte erforderlich ist. Wenn Sie sich in einer älteren Windows-Version mit einem Konto angemeldet haben, das Mitglied der lokalen Gruppe *Administratoren* war, haben Sie automatisch immer Administratorrechte gehabt. Das war eigentlich kein Problem, weil es sowieso empfehlenswert ist, sich nur mit einem Administratorkonto anzumelden, wenn man die Aufgaben eines Administrators wahrnehmen muss. Das Problem besteht darin, dass die Leute dazu neigen, ihr Administratorkonto als normales Benutzerkonto zu verwenden. Das ist bequem, weil man sich nicht ab- und wieder anmelden muss, um Systemverwaltungsarbeiten durchzuführen. Leider ergibt sich aus dieser Verhaltensweise ein Sicherheitsproblem, weil jedes Programm, das von einem Benutzer mit Administratorrechten ausgeführt wird, die Rechte und Berechtigungen dieses Benutzers verwenden kann. Die Benutzerkontensteuerung löst dieses Problem, indem sie es ermöglicht, dass auch ein Mitglied der lokalen Gruppe *Administratoren* den größten Teil der Zeit mit den Rechten eines Standardbenutzers arbeiten kann. Um Verwaltungsarbeiten durchzuführen, kann er seine Rechte kurzfristig anheben und mit den Rechten eines Administrators arbeiten.

Um die Benutzerkontensteuerung zu verstehen, müssen Sie folgende Konzepte kennen:

- **Anhebung der Rechte** Alle Benutzer arbeiten auf einem Windows 7-Client mit den Rechten eines Standardbenutzers. Wenn ein Benutzer versucht, eine Arbeit durchzuführen, für die Administratorrechte erforderlich sind, wie zum Beispiel die Erstellung eines neuen Benutzerkontos, müssen seine Rechte von denen eines Standardbenutzers auf die eines Administrators angehoben werden. Dieser Vorgang wird *Anhebung der*

Rechte genannt (auch *Erhöhung der Rechte*, engl. privilege elevation). Die Benutzerkontensteuerung ist das Mittel zur Anhebung der Rechte. Sie ermöglicht Mitgliedern der lokalen Gruppe *Administratoren* die Arbeit mit Administratorrechten, sorgt aber dafür, dass dies dem betreffenden Benutzer auch bewusst wird. Die Anhebung der Rechte gilt nur für eine bestimmte Aufgabe. Wird in derselben Zeit eine andere Aufgabe durchgeführt, die ebenfalls eine Anhebung der Rechte erfordert, erscheint für diese Aufgabe wieder eine entsprechende Eingabeaufforderung der Benutzerkontensteuerung.

- **Administratorbestätigungsmodus** Im Administratorbestätigungsmodus muss ein Administrator durch die entsprechende Eingabe in der Eingabeaufforderung der Benutzerkontensteuerung seine explizite Zustimmung geben, damit eine Erhöhung der Rechte erfolgen kann. Dazu reicht vielleicht ein Klick auf die Schaltfläche *Ja* aus (*prompting for consent*) oder es müssen Anmeldeinformationen eingegeben werden (*prompting for credentials*). Die erste Art von Eingabeaufforderung könnte man eine Zustimmungsaufforderung nennen, die zweite eine Aufforderung zur Eingabe von Anmeldeinformationen.
- **Sicherer Desktop** Der *sichere Desktop* sorgt dafür, dass Malware nicht die Eingabeaufforderung der Benutzerkontensteuerung ändern kann, um sich auf diese Weise erhöhte Rechte zu verschaffen. Wenn Sie die Benutzerkontensteuerung so konfigurieren, dass sie den sicheren Desktop benutzt, ist der Desktop während der Anzeige der Eingabeaufforderung der Benutzerkontensteuerung nicht zugänglich. Sie müssen auf die Eingabeaufforderung reagieren, bevor Sie wieder mit dem Computer arbeiten können. Der abgeblendete Bildschirm zeigt eine Aufnahme des aktuellen Desktops. Deswegen erscheint ein im Hintergrund laufendes Video im sicheren Desktop wie eingefroren. Wenn Sie nicht innerhalb von 150 Sekunden auf die Eingabeaufforderung der Benutzerkontensteuerung auf dem sicheren Desktop reagieren, lehnt Windows automatisch die Anhebung der Rechte ab und der Computer wechselt wieder zum Standarddesktop.

Einstellungen der Benutzerkontensteuerung

Den Umfang der Benachrichtigungen durch die Benutzerkontensteuerung können Sie selbst im Dialogfeld *Einstellungen für Benutzerkontensteuerung* einstellen (Abbildung 9.1). Um dieses Dialogfeld zu öffnen, klicken Sie auf der Seite *Benutzerkonten* der Systemsteuerung auf das Element *Einstellungen der Benutzerkontensteuerung ändern*. Das Dialogfeld enthält einen Schieberegler, mit dem Sie Einstellungen von *Nie benachrichtigen* bis *Immer benachrichtigen* vornehmen können.

Wenn Sie die Einstellung ändern, werden Sie von der Benutzerkontensteuerung darüber informiert, dass ein Programm namens UserAccountControlSettings versucht, auf Ihrem Computer eine Änderung vorzunehmen (Abbildung 9.2). Dieses Dialogfeld ist eine Sicherheitsmaßnahme, die dafür sorgt, dass Malware die Einstellungen für die Benutzerkontensteuerung nicht ändern kann, ohne dass Sie davon erfahren. Wenn Sie diese Meldung sehen und die Einstellungen nicht selbst geändert haben, ist es sehr wahrscheinlich, dass Malware versucht, sich an Ihrem Computer zu schaffen zu machen.

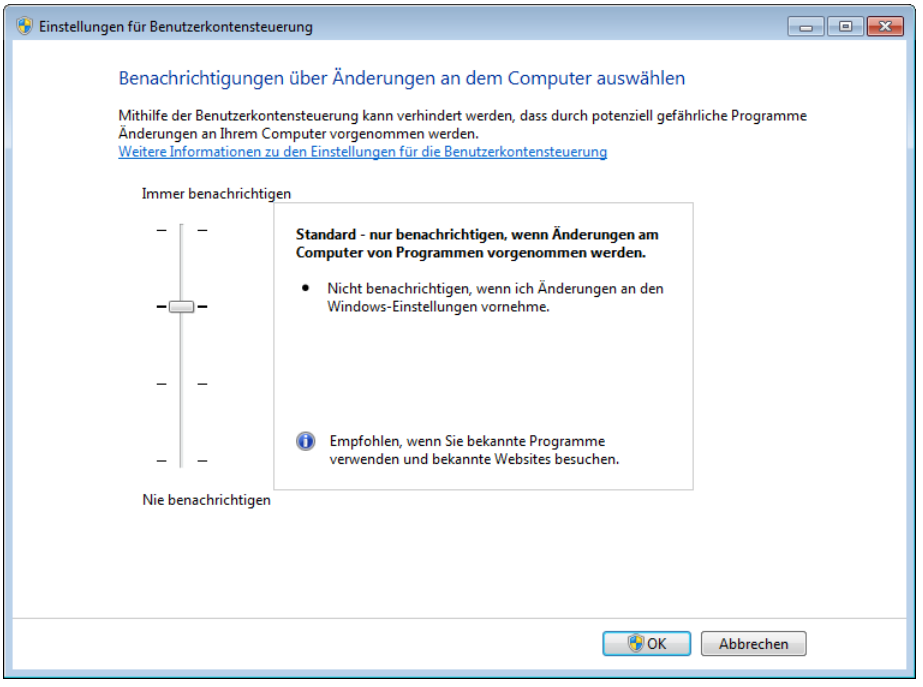

Einstellungen für Benutzerkontensteuerung
Benachrichtigungen über Änderungen an dem Computer auswählen
Mithilfe der Benutzerkontensteuerung kann verhindert werden, dass durch potenziell gefährliche Programme Änderungen an Ihrem Computer vorgenommen werden.
Weitere Informationen zu den Einstellungen für die Benutzerkontensteuerung
Immer benachrichtigen
Standard - nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden.
Nicht benachrichtigen, wenn ich Änderungen an den Windows-Einstellungen vornehme.
Empfohlen, wenn Sie bekannte Programme verwenden und bekannte Websites besuchen.
Nie benachrichtigen
OK
Abbrechen

Abbildung 9.1 *Einstellungen für Benutzerkontensteuerung*

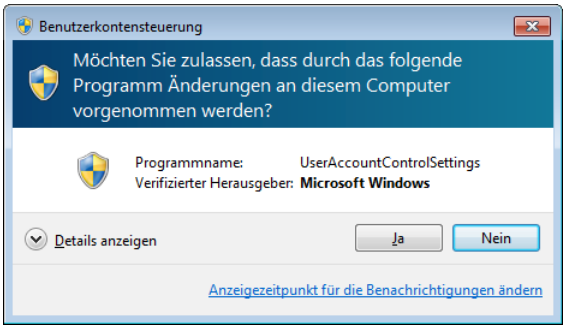


Abbildung 9.2 Eine Warnung vor der Änderung der Einstellungen für die Benutzerkontensteuerung

Mit diesem Schieberegler können Sie folgende Einstellungen vornehmen:

- **Immer benachrichtigen** Das ist die sicherste Einstellung. Sie werden informiert, bevor Programme Änderungen am Computer oder an den Windows-Einstellungen durchführen, für die Administratorrechte erforderlich sind. Während der Benachrichtigung wird der Desktop abgeblendet dargestellt, weil der sichere Desktop aktiv geworden ist. Sie müssen auf die Eingabeaufforderung reagieren, um mit dem Computer weiterarbeiten zu können. Wenn Sie nicht innerhalb von 150 Sekunden reagieren, verweigert Windows automatisch die Anhebung der Rechte und der Computer wechselt wieder zum Standarddesktop.

- **Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden** Bei dieser Einstellung werden Sie informiert, bevor Programme Änderungen am Computer oder an den Windows-Einstellungen durchführen, für die Administratorrechte erforderlich sind. Die Benachrichtigung erfolgt auf dem sicheren Desktop. Wenn Sie nicht innerhalb von 150 Sekunden reagieren, verweigert Windows automatisch die Anhebung der Rechte.
- **Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden (Desktop nicht abblenden)** Bei dieser Einstellung werden Sie informiert, bevor Programme Änderungen durchführen, für die Administratorrechte erforderlich sind. Sie werden nicht informiert, wenn Sie mit Programmen aus dem Lieferumfang von Windows Änderungen an den Windows-Einstellungen durchführen, für die Administratorrechte erforderlich sind. Sie werden informiert, wenn ein Programm, das nicht zum Lieferumfang von Windows gehört, Windows-Einstellungen zu ändern versucht.
- **Nie benachrichtigen** Wenn Sie als Administrator angemeldet sind, werden Sie nicht informiert, wenn Programme Änderungen am Computer oder an Windows-Einstellungen durchführen. Wenn Sie als Standardbenutzer angemeldet sind, werden alle Änderungen, für die Administratorrechte erforderlich sind, automatisch abgelehnt.

Schnelltest

- Was ist der Unterschied zwischen den Einstellungen *Immer benachrichtigen* und *Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden (Desktop nicht abblenden)*?

Antwort zum Schnelltest

- Bei der Einstellung *Immer benachrichtigen* wird die Eingabeaufforderung auf dem sicheren Desktop angezeigt. Dann können Sie erst weiterarbeiten, nachdem Sie auf die Eingabeaufforderung reagiert haben. Bei der Einstellung *Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden (Desktop nicht abblenden)* können Sie weiterarbeiten, während die Eingabeaufforderung der Benutzerkontensteuerung noch geöffnet ist.

Richtlinien für die Benutzerkontensteuerung

Die Konfiguration der Benutzerkontensteuerung erfolgt hauptsächlich durch Gruppenrichtlinien. Die Richtlinien für die Benutzerkontensteuerung liegen alle im Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen*. Es gibt 10 Richtlinien, deren Namen alle mit dem Präfix Benutzerkontensteuerung beginnen (Abbildung 9.3).

In den nächsten Abschnitten erfahren Sie mehr über diese Richtlinien und ihre Wirkung auf die Benutzerkontensteuerung.

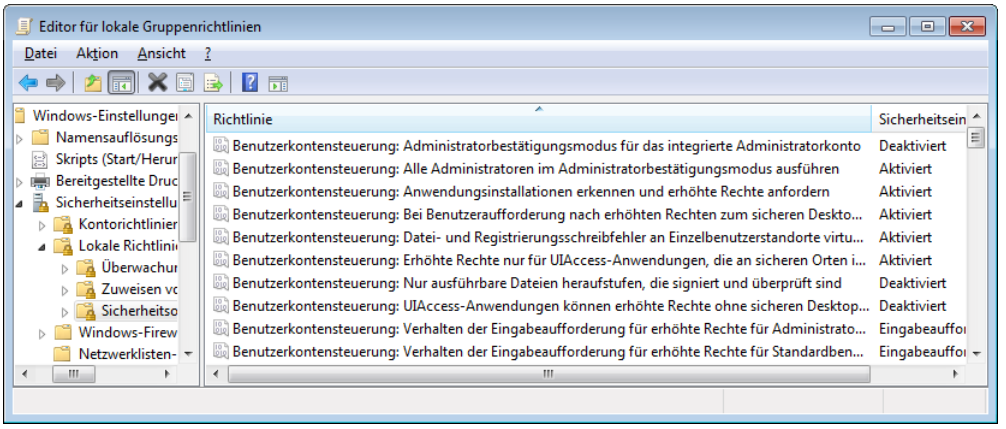


Abbildung 9.3 Richtlinien für die Benutzerkontensteuerung

Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto

Die Richtlinie *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto* steuert das Verhalten des Administratorbestätigungsmodus für das vordefinierte *Administrator*-Konto. Standardmäßig ist das vordefinierte *Administrator*-Konto deaktiviert. Diese Richtlinie ist also nur von Bedeutung, wenn Sie das vordefinierte *Administrator*-Konto mit der Richtlinie *Konten: Administratorkontostatus* aktiviert haben, die ebenfalls im Knoten *Sicherheitsoptionen* zu finden ist. Die Standardeinstellung dieser Richtlinie ist *Deaktiviert*. Wenn Sie das vordefinierte *Administrator*-Konto aktivieren, erfolgt automatisch eine Anhebung der Rechte ohne Eingabeaufforderung der Benutzerkontensteuerung. Wenn Sie diese Richtlinie und das vordefinierte *Administrator*-Konto aktivieren, werden für das vordefinierte Konto Eingabeaufforderungen der Benutzerkontensteuerung angezeigt, wenn mit dem Konto Aufgaben durchgeführt werden, die eine Anhebung der Rechte erfordern.

Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus

Die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* funktioniert so ähnlich wie das Dialogfeld *Einstellungen für Benutzerkontensteuerung*, das in dieser Lektion bereits besprochen wurde. Damit können Sie festlegen, in welchem Umfang sich die Benutzerkontensteuerung bei Benutzern melden soll, die sich mit Administratorrechten auf einem Windows 7-Client anmelden. Während das Dialogfeld *Einstellungen für Benutzerkontensteuerung* aber nur über vier Einstellungen verfügt, sind in der Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* sechs Einstellungen möglich (Abbildung 9.4).

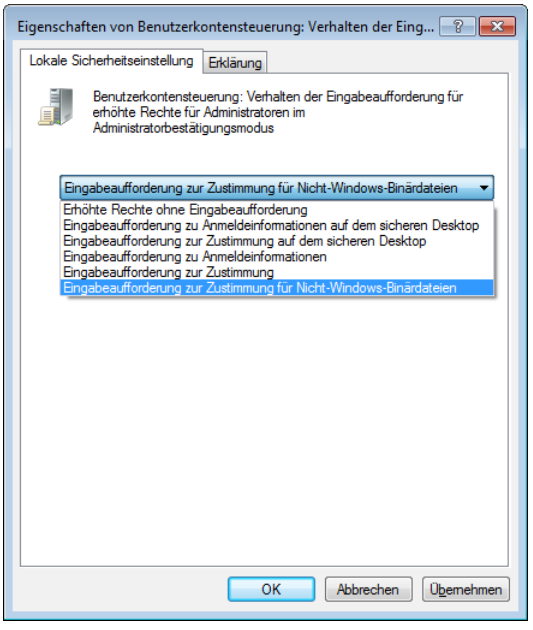

Eigenschaften von Benutzerkontensteuerung: Verhalten der Eing...
Lokale Sicherheitseinstellung
Erklärung
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus
Eingabeaufforderung zur Zustimmung für Nicht-Windows-Binärdateien
Erhöhte Rechte ohne Eingabeaufforderung
Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop
Eingabeaufforderung zur Zustimmung auf dem sicheren Desktop
Eingabeaufforderung zu Anmeldeinformationen
Eingabeaufforderung zur Zustimmung
Eingabeaufforderung zur Zustimmung für Nicht-Windows-Binärdateien
OK
Abbrechen
Übernehmen

Abbildung 9.4 Einstellungen für die Benutzerkontensteuerung für Administratoren

Die Einstellungen haben folgende Auswirkungen:

- **Erhöhte Rechte ohne Eingabeaufforderung** Das ist die unsicherste Einstellung. Sie entspricht einer Deaktivierung der Benutzerkontensteuerung. Anforderungen für eine Anhebung der Rechte werden automatisch genehmigt.
- **Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop** Die Benutzerkontensteuerung fordert den Administrator auf dem sicheren Desktop zur Eingabe eines Kennworts auf (Abbildung 9.5).

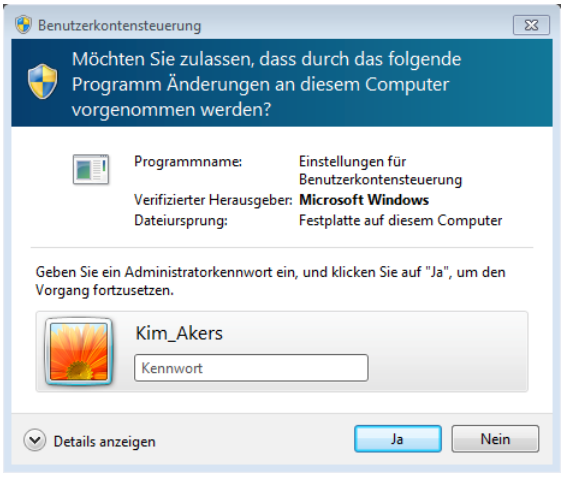

Benutzerkontensteuerung
Möchten Sie zulassen, dass durch das folgende Programm Änderungen an diesem Computer vorgenommen werden?
Programmname: Einstellungen für Benutzerkontensteuerung
Verifizierter Herausgeber: Microsoft Windows
Dateiursprung: Festplatte auf diesem Computer
Geben Sie ein Administratorkennwort ein, und klicken Sie auf "Ja", um den Vorgang fortzusetzen.
Kim_Akers
Kennwort
Details anzeigen
Ja
Nein

Abbildung 9.5 Eingabeaufforderung zu Anmeldeinformationen

- **Eingabeaufforderung zur Zustimmung auf dem sicheren Desktop** Die Benutzerkontensteuerung fordert den Administrator auf dem sicheren Desktop zu seiner Zustimmung auf (Abbildung 9.6). Diese Einstellung erfordert keine Eingabe eines Kennworts.

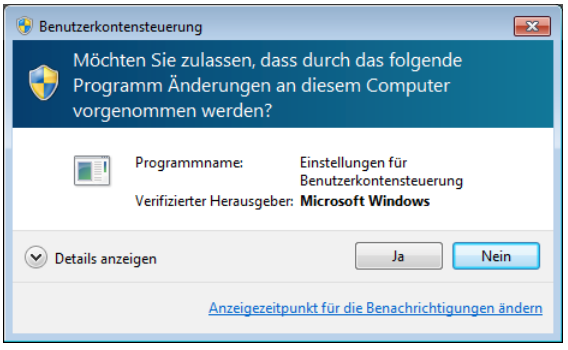


Abbildung 9.6 Zustimmungsaufforderung

- **Eingabeaufforderung zu Anmeldeinformationen** Der Benutzer muss ein Kennwort eingeben. Der sichere Desktop wird nur verwendet, wenn die Richtlinie *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln* aktiviert ist (die Standardeinstellung dieser Richtlinie).
- **Eingabeaufforderung zur Zustimmung** Diese Richtlinie fordert zur Zustimmung auf. Der sichere Desktop wird nur verwendet, wenn die Richtlinie *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln* aktiviert ist (die Standardeinstellung dieser Richtlinie).
- **Eingabeaufforderung zur Zustimmung für Nicht-Windows-Binärdateien** Die Standardeinstellung der Richtlinie. Die Benutzerkontensteuerung meldet sich nur, wenn eine Anwendung eine Rechteanhebung anfordert, die nicht zum Windows-Betriebssystem gehört. Anwendungen, die zum Windows-Betriebssystem gehören und eine Rechteanhebung anfordern, lösen keine Eingabeaufforderung der Benutzerkontensteuerung aus.

Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer

Die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer* legt fest, ob und wie ein Benutzer, der kein Administrator ist, über die Anforderung nach einer Anhebung der Rechte informiert wird (Abbildung 9.7). Die Einstellung *Anforderungen für erhöhte Rechte automatisch ablehnen* führt zur automatischen Ablehnung einer angeforderten Rechteerhöhung. Windows weist den Benutzer nicht direkt auf die Ablehnung hin, aber der Benutzer stellt natürlich fest, dass er die Arbeit nicht durchführen kann, die diese Eingabeaufforderung ausgelöst hat. Die anderen Optionen sind *Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop* und die Standardeinstellung *Eingabeaufforderung zu Anmeldeinformationen*. Anmeldeinformationen sind erforderlich, weil die Rechteerhöhung von einem Benutzer genehmigt werden muss, der über Administratorrechte verfügt.

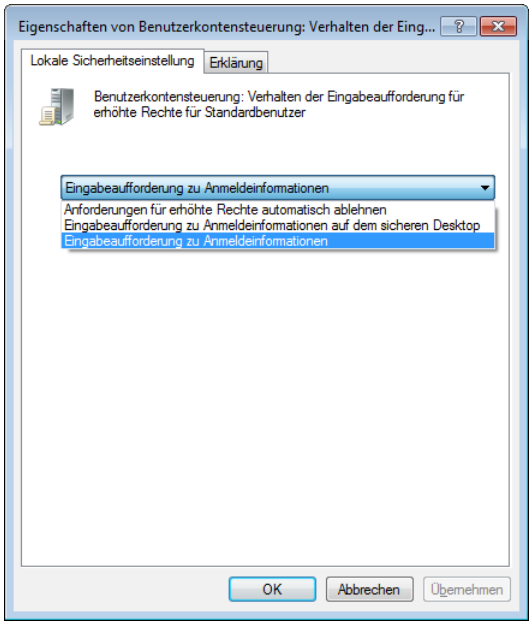


Abbildung 9.7 Einstellen des Verhaltens der Benutzerkontensteuerung für Standardbenutzer

Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern

Die Richtlinie *Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern* legt fest, ob das Installationsprogramm einer Anwendung eine Anhebung der Rechte anfordern kann. Die Standardeinstellung ist *Aktiviert*. Somit wird die Softwareinstallation zugelassen, wenn eine Zustimmung gegeben oder die erforderlichen Anmeldeinformationen eingegeben werden. In Unternehmensumgebungen, in denen Software über Gruppenrichtlinien verteilt wird und die direkte Verwendung von Installationsprogrammen unnötig ist, wird diese Richtlinie meistens deaktiviert.

Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind

Wenn Sie die Richtlinie *Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind* aktivieren, zeigt die Benutzerkontensteuerung nur für ausführbare Dateien eine Eingabeaufforderung zur Rechteanhebung an, die mit einem Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert wurden. Wurde die Anwendung nicht signiert oder wird das Zertifikat nicht als vertrauenswürdig eingestuft, lässt die Benutzerkontensteuerung keine Anhebung der Rechte zu. Standardmäßig ist diese Richtlinie deaktiviert und sie sollte nur in Umgebungen verwendet werden, in denen alle Anwendungen, die eine Anhebung der Rechte erfordern, digital signiert sind.

Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen

Die Richtlinie *Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen* legt fest, ob Windows für alle Benutzer mit Administratorrechten die Be-

nutzerkontensteuerung verwendet, wenn sie Arbeiten durchführen, für die eine Anhebung der Rechte erforderlich ist. Die Standardeinstellung dieser Richtlinie ist *Aktiviert*. Wird die Richtlinie deaktiviert, erhalten alle Benutzer mit Administratorrechten automatisch erhöhte Rechte, wenn sie eine Arbeit durchführen, für die erhöhte Rechte erforderlich sind. Eine Deaktivierung dieser Richtlinie deaktiviert die Benutzerkontensteuerung für alle Benutzer mit Administratorrechten.

Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln

Die Richtlinie *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln* legt fest, ob die Eingabeaufforderung der Benutzerkontensteuerung auf dem sicheren Desktop angezeigt wird, wenn eine Erhöhung der Rechte erforderlich ist. Auf dem sicheren Desktop wird der normale Desktop in abgeblendeter Form angezeigt und der Benutzer muss auf die Eingabeaufforderung reagieren, bevor er wieder mit dem Computer arbeiten kann. Das ist eine Sicherheitsmaßnahme, die verhindert, dass Malware die Eingabeaufforderung der Benutzerkontensteuerung nachahmt und durch diesen Trick unerkannt eine Zustimmung erhält. Die Richtlinie wird standardmäßig aktiviert. Wenn Sie diese Richtlinie deaktivieren und die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* auf *Eingabeaufforderung zur Zustimmung auf dem sicheren Desktop* oder *Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop* eingestellt wird, wird trotzdem der sichere Desktop verwendet.

Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren

Viele ältere Anwendungen versuchen, Daten in die Ordner *Programme*, *Windows* oder *Windows\System32* oder in den Bereich *HKLM\SOFTWARE* der Registrierung zu schreiben. Windows 7 erlaubt Anwendungen nicht, Daten an diese sicheren Orte zu schreiben. Damit diese Anwendungen trotzdem ausgeführt werden können, leitet Windows 7 die entsprechenden Schreibzugriffe auf benutzerbezogene virtualisierte Orte um, wobei die Anwendungen davon ausgehen, die Daten erfolgreich geschrieben zu haben. Wird die Richtlinie *Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren* deaktiviert, blockiert Windows Schreibzugriffe der Anwendungen an sicheren Orten. Die Richtlinie ist standardmäßig aktiviert.

Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern

UIAccess-Anwendungen (User Interface Accessibility) sind spezielle Programme, die für einen Benutzer mit Windows interagieren können, wie zum Beispiel die Bildschirmtastatur und Windows-Remoteunterstützung. Die Richtlinie *Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern* legt fest, ob UIAccess-Anwendungen, die durch ihre Eigenschaften als solche zu erkennen sind, eine Anhebung der Rechte anfordern können, ohne einen Wechsel zum sicheren Desktop auszulösen. Die Standardeinstellung dieser Richtlinie ist *Deaktiviert*.

Sie sollten diese Richtline aktivieren, wenn Helfer auf Eingabeaufforderungen der Benutzerkontensteuerung reagieren müssen, die während einer Remoteunterstützungssitzung auftreten. Wird in einer Remoteunterstützungssitzung eine Eingabeaufforderung der Benutzer-

kontensteuerung ausgelöst, erscheint sie normalerweise auf dem sicheren Desktop. Für Helfer ist dieser sichere Desktop aber nicht zugänglich, wenn sie über eine Remoteunterstützungssitzung verbunden sind. Ein Helfer kann nur dann auf die Eingabeaufforderung reagieren, wenn bei der Verwendung von UIAccess-Anwendungen kein sicherer Desktop verwendet wird. Diese Richtlinie ist nur erforderlich, wenn Eingabeaufforderungen der Benutzerkontensteuerung für Standardbenutzer konfiguriert wurden. Wenn die Richtlinie nicht aktiviert wird, ist für Standardbenutzer keine Anhebung der Rechte möglich. Der Helfer erhält also gar nicht die Gelegenheit, Anmeldeinformationen einzugeben.

Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind

Die Richtlinie *Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind* gilt nur für Anwendungen, die eine Ausführung auf der UIAccess-Integritätsstufe anfordern. Die Standardeinstellung für diese Richtlinie ist *Aktiviert*. Das bedeutet, dass nur Anwendungen, die in den Ordnern *Windows\System32* und *Programme* und deren Unterordnern installiert wurden, mit dieser speziellen Integritätsstufe ausgeführt werden können. Programme, die eine Ausführung mit UIAccess-Integrität anfordern, müssen unabhängig von dieser Richtlinieneinstellung mit einem vertrauenswürdigen Zertifikat signiert worden sein.

Secpol und die Konsole *Lokale Sicherheitsrichtlinie*

Die Konsole *Lokale Sicherheitsrichtlinie* (*Secpol.msc*, Abbildung 9.8) ist im Abschnitt *System und Sicherheit/Verwaltung* der Systemsteuerung zu finden. Die Konsole zeigt eine Teilmenge der Richtlinien an, die im Editor für lokale Gruppenrichtlinien verfügbar sind. Mit der Konsole *Lokale Sicherheitsrichtlinie* können Sie die Richtlinien bearbeiten, die im Editor für lokale Gruppenrichtlinien im Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen* angezeigt werden. Der Vorteil der Konsole *Lokale Sicherheitsrichtlinie* besteht darin, dass sie auf Sicherheitseinstellungen spezialisiert ist. Jede Aufgabe, die Sie in der Konsole *Lokale Sicherheitsrichtlinie* durchführen können, lässt sich auch im Editor für lokale Gruppenrichtlinien durchführen.

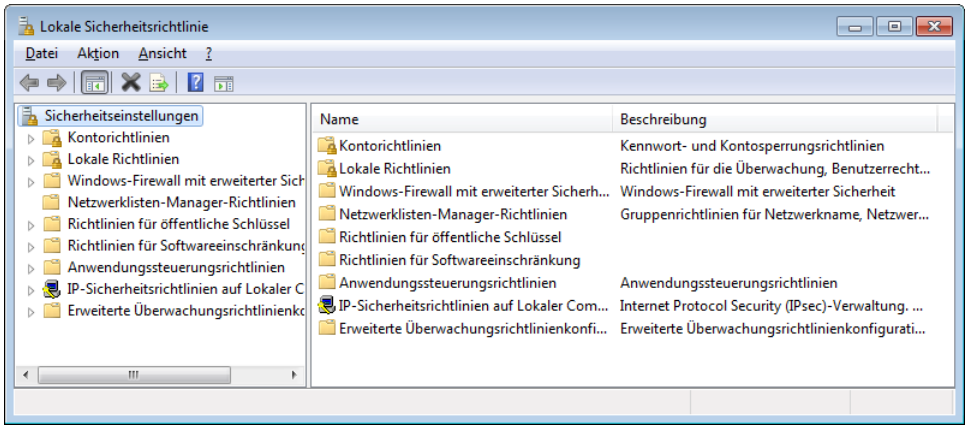


Abbildung 9.8 Die Konsole *Lokale Sicherheitsrichtlinie*

Sicherheitsspezifische Gruppenrichtlinieneinstellungen können Sie mit dem Editor für lokale Gruppenrichtlinien und mit der Konsole *Lokale Sicherheitsrichtlinie* importieren und exportieren. Auf diese Weise können Sie eigenständige Computer, die nicht zu einer Domäne gehören, mit denselben Sicherheitseinstellungen versorgen. Exportierte Sicherheitsrichtlinien werden im Security Template-Format als *.inf*-Datei gespeichert. Solche Dateien können Sie nicht nur mit dem Editor für lokale Gruppenrichtlinien und der Konsole *Lokale Sicherheitsrichtlinie* importieren, sondern auch mit dem Befehlszeilenprogramm *Secedit.exe*. In der folgenden Übung verwenden Sie den Editor für lokale Gruppenrichtlinien.



Prüfungstipp

Merken Sie sich den Unterschied zwischen einer Eingabeaufforderung zur Zustimmung und einer Eingabeaufforderung für Anmeldeinformationen.

Übung Konfigurieren der Benutzerkontensteuerung

Die Benutzerkontensteuerung lässt sich konfigurieren, um den Vorstellungen der Administratoren und Benutzer besser zu entsprechen. In diesen Übungen nehmen Sie verschiedene Einstellungen für die Benutzerkontensteuerung vor und überprüfen die Wirkung, um eine bessere Vorstellung davon zu bekommen, welche Konfigurationsoptionen verfügbar sind.

Übung 1 Einstellungen für die Benutzerkontensteuerung

In dieser Übung nehmen Sie Einstellungen für die Benutzerkontensteuerung vor und überprüfen die Wirkung.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Benutzerkonten** ein**.** Klicken Sie im Startmenü auf das Element *Benutzerkonten*.
3. Klicken Sie auf das Element *Anderes Konto verwalten*. Sie werden nicht von der Benutzerkontensteuerung aufgefordert, den Wechsel auf die Seite *Konten verwalten* zu bestätigen. Klicken Sie auf *Zur Hauptseite für Benutzerkonten wechseln*.
4. Klicken Sie auf das Element *Einstellungen der Benutzerkontensteuerung ändern*. Auch diesmal meldet sich die Benutzerkontensteuerung nicht.
5. Schieben Sie den Schieber auf der Seite *Benachrichtigungen über Änderungen an dem Computer auswählen* in die Position *Immer benachrichtigen*. Klicken Sie auf *OK*.
6. Klicken Sie in der Eingabeaufforderung der Benutzerkontensteuerung auf *Ja*.
7. Klicken Sie auf das Element *Anderes Konto verwalten*. Diesmal werden Sie von der Benutzerkontensteuerung aufgefordert, den Wechsel auf die Seite *Konten verwalten* zu bestätigen. Der Bildschirm wird dabei abgeblendet, um darauf hinzuweisen, dass der sichere Desktop aktiv ist. Klicken Sie auf *Nein*, um die Eingabeaufforderung der Benutzerkontensteuerung zu schließen.
8. Klicken Sie auf das Element *Einstellungen der Benutzerkontensteuerung ändern*. Diesmal erfolgt ein Wechsel zum sicheren Desktop und die Benutzerkontensteuerung fordert Sie zu einer Bestätigung auf. Klicken Sie auf *Ja*.
9. Schieben Sie den Schieber auf der Seite *Benachrichtigungen über Änderungen an dem Computer auswählen* wieder in die Position *Standard – nur benachrichtigen, wenn*

Änderungen am Computer von Programmen vorgenommen werden. Klicken Sie auf *OK*. Klicken Sie auf *Ja*, wenn sich die Benutzerkontensteuerung meldet.

10. Schließen Sie die Systemsteuerung.

Übung 2 Konfigurieren und Exportieren von Benutzerkontensteuerungsrichtlinien

In dieser Übung nehmen Sie im Editor für lokale Gruppenrichtlinien Einstellungen für die Benutzerkontensteuerung vor.

1. Sofern Sie es noch nicht getan haben, melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Erstellen Sie im Windows-Explorer den Ordner *C:\Export*.
3. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Gruppenrichtlinie bearbeiten** ein. Klicken Sie auf das Element *Gruppenrichtlinie bearbeiten*.
4. Sorgen Sie dafür, dass der Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen* gewählt ist. Öffnen Sie das Menü *Aktion* und wählen Sie dann *Richtlinie exportieren*.
5. Speichern Sie die exportierte Richtlinie als *C:\Export\Richtliniengrundeinstellungen.inf*.
6. Wählen Sie in den Sicherheitseinstellungen den Knoten *Lokale Richtlinien\Sicherheitsoptionen*. Klicken Sie die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* mit einem Doppelklick an.
7. Wählen Sie die Einstellung *Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop* (Abbildung 9.9) und klicken Sie dann auf *OK*.

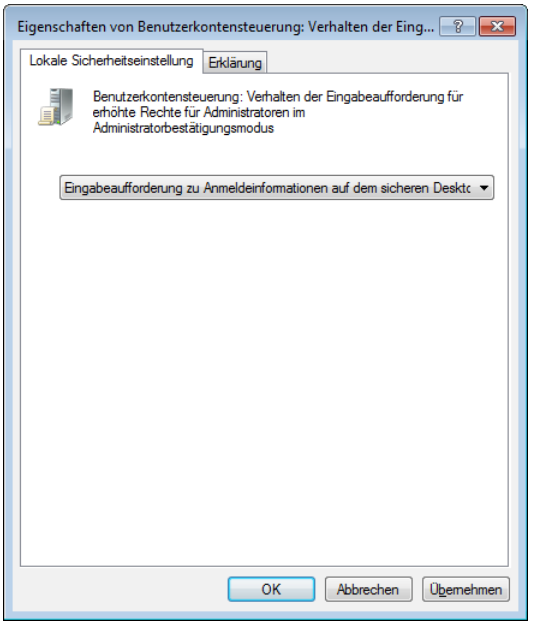


Abbildung 9.9 *Eingabeaufforderung zu Anmeldeinformationen auf dem sicheren Desktop*

8. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* den Befehl **gpupdate /force** ein und drücken Sie die EINGABETASTE.
9. Klicken Sie auf *Start*. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Benutzerkonten** ein. Klicken Sie im Startmenü auf das Element *Benutzerkonten*.
10. Klicken Sie auf das Element *Einstellungen der Benutzerkontensteuerung ändern*. Nun müssen Sie in diesem Fall auf dem sicheren Desktop Ihr Kennwort eingeben (Abbildung 9.10). Geben Sie das Kennwort ein und klicken Sie dann auf *Ja*.

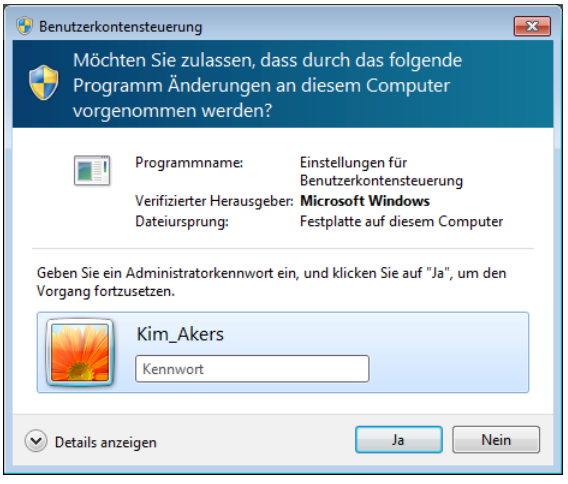


Abbildung 9.10 Eingeben der Anmeldeinformationen

11. Der Schieber im Dialogfeld *Einstellungen für Benutzerkontensteuerung* steht nun in der sichersten Position und nicht mehr in der Standardposition, auf die Sie ihn in der vorigen Übung gestellt haben. Klicken Sie auf *Abbrechen*, um das Dialogfeld zu schließen.
12. Sorgen Sie dafür, dass der Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen* gewählt ist. Öffnen Sie das Menü *Aktion* und klicken Sie dann auf *Richtlinie importieren*. Importieren Sie die Richtliniendatei *C:\Export\Richtliniengrundeinstellungen.inf*. Wenn Sie eine Fehlermeldung erhalten, klicken Sie auf *OK*.
13. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **gpupdate /force** ein.
14. Klicken Sie auf der Seite *Benutzerkonten* der Systemsteuerung auf das Element *Einstellungen der Benutzerkontensteuerung ändern*. Das Dialogfeld *Einstellungen für Benutzerkontensteuerung* öffnet sich, ohne dass Sie Ihr Kennwort eingeben müssen. Außerdem steht der Schieber wieder in der Standardposition.
15. Schließen Sie alle geöffneten Fenster und melden Sie sich ab.

Zusammenfassung der Lektion

- Zur Bearbeitung von sicherheitsspezifischen Gruppenrichtlinien können Sie die Konsole *Lokale Sicherheitsrichtlinie* oder den Editor für lokale Gruppenrichtlinien verwenden.
- Wird die Benutzerkontensteuerung so eingestellt, dass sie den sicheren Desktop benutzt, muss ein Administrator auf die Eingabeaufforderung reagieren, um wieder mit dem Computer arbeiten zu können.
- Die Benutzerkontensteuerung kann mit einer Eingabeaufforderung zur Zustimmung oder einer Eingabeaufforderung für Anmeldeinformationen konfiguriert werden. In einer Zustimmungsaufforderungen braucht der Administrator die Erhöhung der Rechte nur zu bestätigen. In einer Aufforderung zur Eingabe von Anmeldeinformationen muss der Administrator sein Kennwort eingeben, um die Erhöhung der Rechte zu bestätigen.
- Standardmäßig erhalten Standardbenutzer unter Windows 7 keine Eingabeaufforderung der Benutzerkontensteuerung. Sie können die Benutzerkontensteuerung so konfigurieren, dass Standardbenutzer zur Eingabe von Anmeldeinformationen aufgefordert werden. Dann müssen sie die Anmeldeinformationen eines Benutzers eingeben, der Mitglied der lokalen Gruppe *Administratoren* ist.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Verwalten der Benutzerkontensteuerung«, überprüfen. Die Fragen sind (in englischer Sprache) auch auf der Begleit-CD zu finden, falls Sie die elektronische Form der Fragen vorziehen.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welche Richtlinieneinstellung müssen Sie vornehmen, wenn ein Benutzer, der unter Windows 7 das vordefinierte *Administrator*-Konto verwendet, eine Eingabeaufforderung der Benutzerkontensteuerung erhalten soll, bevor die Rechte angehoben werden?
   A. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus*: *Erhöhte Rechte ohne Eingabeaufforderung*
   B. *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto: Aktiviert*
   C. *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto: Deaktiviert*
   D. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus*: *Eingabeaufforderung zur Zustimmung für Nicht-Windows-Binärdateien*

2. Welche der folgenden Richtlinieneinstellungen sollten Sie vornehmen, damit Benutzer, die auf einem Windows 7-Client nicht Mitglieder der lokalen Gruppe *Administratoren* sind, zur Eingabe von Anmeldeinformationen aufgefordert werden, wenn sie eine Arbeit durchführen, die eine Erhöhung der Rechte erfordert?
   A. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer: Anforderungen für erhöhte Rechte automatisch ablehnen*
   B. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer: Eingabeaufforderung zu Anmeldeinformationen*
   C. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus: Eingabeaufforderung zu Anmeldeinformationen*
   D. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus: Eingabeaufforderung zur Zustimmung*
3. Sie leiten einen Computerkurs, der mit 30 eigenständigen Windows 7-Computern ausgestattet ist. Die Computer sind zwar nicht Mitglieder einer Domäne, gehören aber zur selben Heimnetzgruppe. Auf einem Referenzcomputer haben Sie einige Richtlinien für die Benutzerkontensteuerung konfiguriert. Nun möchten Sie diese Einstellungen auf die 30 Computer übertragen. Welche der folgenden Tools können Sie verwenden? (Wählen Sie alle zutreffenden Antworten.)
   A. Die Konsole *Editor für lokale Gruppenrichtlinien*
   B. Die Konsole *Computerverwaltung*
   C. Das Dialogfeld *Einstellungen für Benutzerkontensteuerung*
   D. Die Konsole *Lokale Sicherheitsrichtlinie*
4. In Ihrer Organisation sind Sie mit der Ausmusterung älterer Anwendungen beschäftigt. Sie möchten sicherstellen, dass ältere Anwendungen, die Daten an sichere Orte schreiben, beispielsweise in den Ordner *\Windows\System32*, damit keinen Erfolg haben und nicht von Windows an einen anderen Ort umgeleitet werden. Mit welcher der folgenden Richtlinien erreichen Sie dies?
   A. *Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind*
   B. *Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind*
   C. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer*
   D. *Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren*
5. Sie möchten zwar, dass Mitglieder der lokalen Gruppe *Administratoren* eine Aufforderung zur Eingabe von Anmeldeinformationen erhalten, wenn sie Arbeiten durchführen wollen, für die eine Erhöhung der Rechte erforderlich ist, aber es soll kein Wechsel zum sicheren Desktop erfolgen. Sie haben die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* auf *Eingabeaufforderung zu Anmeldeinformationen* eingestellt. Für Mitglieder der lokalen Gruppe *Administratoren* erfolgt aber ein Wechsel

zum sicheren Desktop, wenn die Eingabeaufforderung angezeigt wird. Mit welcher der folgenden Richtlinien lösen Sie das Problem?

A. *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto*

B. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus*

C. *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln*

D. *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer*

Lektion 2: Windows 7-Authentifizierung und -autorisierung

Wenn ein Benutzer sein Kennwort vergisst, kann er sich nicht mehr an seinem Computer anmelden. Und wenn er sich nicht mehr an seinem Computer anmelden kann, kann er seine Arbeit nicht erledigen. In dieser Lektion erfahren Sie etwas über die Lösungen, die Windows 7 für das Problem des vergessenen Kennworts bietet, angefangen von der vorausschauenden Erstellung einer Kennwortrücksetzdiskette bis hin zur Rücksetzung des Kennworts durch ein Mitglied der lokalen Administratorengruppe. Kennwörter sind auf einem Windows 7-Computer nicht die einzige Möglichkeit zur Authentifizierung. Windows 7 unterstützt eine mehrstufige Authentifizierung, und zwar hauptsächlich mithilfe von Treibern, die den PIV-Smartcardstandard (Personal Identity Verification) unterstützen, sowie durch Richtlinien, mit denen sich festlegen lässt, dass zur Anmeldung eine Smartcard erforderlich ist. Außerdem erfahren Sie in dieser Lektion etwas über die Anmeldeinformationsverwaltung, mit der Sie gespeicherte Anmeldeinformationen, wie sie beispielsweise zur Anmeldung bei Websites und Terminalservern erforderlich sind, verwalten, sichern und wiederherstellen können. Zum Stoff dieser Lektion gehört auch die Zuweisung von Benutzerrechten und die Konfiguration von Kennwortrichtlinien.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Sichern und Wiederherstellen von Anmeldeinformationen mit der Anmeldeinformationsverwaltung
- Verwalten von Zertifikaten mit dem Zertifikatmanager
- Verwenden von Runas zur Ausführung von Befehlen mit anderen Anmeldeinformationen
- Konfigurieren von Konten- und Smartcardrichtlinien
- Beheben von Authentifizierungsproblemen

Veranschlagte Zeit für diese Lektion: 40 Minuten

Anmeldeinformationsverwaltung

Die Anmeldeinformationsverwaltung speichert Benutzernamen und Kennwörter, die zur Anmeldung bei Netzwerkressourcen wie Dateiservern, Websites und Terminalservern verwendet werden. Diese Daten werden im Windows-Tresor verwaltet. Sie können den Windows-Tresor sichern und auf einem anderen Windows 7-Computer wiederherstellen. Auf diese Weise lassen sich gespeicherte Anmeldeinformationen auf andere Computer übertragen. Die Anmeldeinformationsverwaltung kann zwar bestimmte Arten von digitalen Zertifikaten sichern, aber sie eignet sich nicht zur Sicherung und Wiederherstellung von selbstsignierten EFS-Zertifikaten (Encrypting File System), wie sie Windows 7 automatisch generiert, wenn Sie eine Datei verschlüsseln. Daher müssen Sie EFS-Zertifikate mit anderen Tools sichern, wie es im Verlauf dieser Lektion noch ausführlicher beschrieben wird.

Wie Abbildung 9.11 zeigt, ist es möglich, Anmeldeinformationen im Windows-Tresor zu speichern, indem man im Dialogfeld *Windows-Sicherheit* das Kontrollkästchen *Anmeldedaten speichern* wählt. Wenn Sie sich im Windows Internet Explorer, im Windows-Explorer oder bei einer Remotedesktopverbindung für die Speicherung Ihrer Anmeldeinformationen entscheiden, überträgt die Anmeldeinformationsverwaltung diese Daten in den Windows-Tresor.

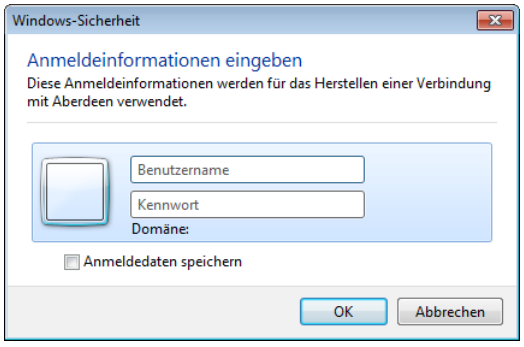


Abbildung 9.11 *Anmeldedaten speichern*

Sie können Anmeldeinformationen für Ressourcen auch zum Windows-Tresor hinzufügen, bevor Sie die Ressourcen tatsächlich verwenden. So fügen Sie Anmeldeinformationen zum Windows-Tresor hinzu:

1. Öffnen Sie die Anmeldeinformationsverwaltung. Dazu geben Sie im Textfeld *Programme/Dateien durchsuchen* des *Start*-Menüs **Anmeldeinformationsverwaltung** ein und klicken dann im *Start*-Menü auf *Anmeldeinformationsverwaltung*.
2. Klicken Sie auf das Element *Windows-Anmeldeinformationen hinzufügen*.
3. Geben Sie im Dialogfeld *Windows-Anmeldeinformationen hinzufügen* die Internet- oder Netzwerkadresse, den Benutzernamen und das Kennwort der Anmeldeinformationen ein, die Sie im Windows-Tresor speichern möchten (Abbildung 9.12).

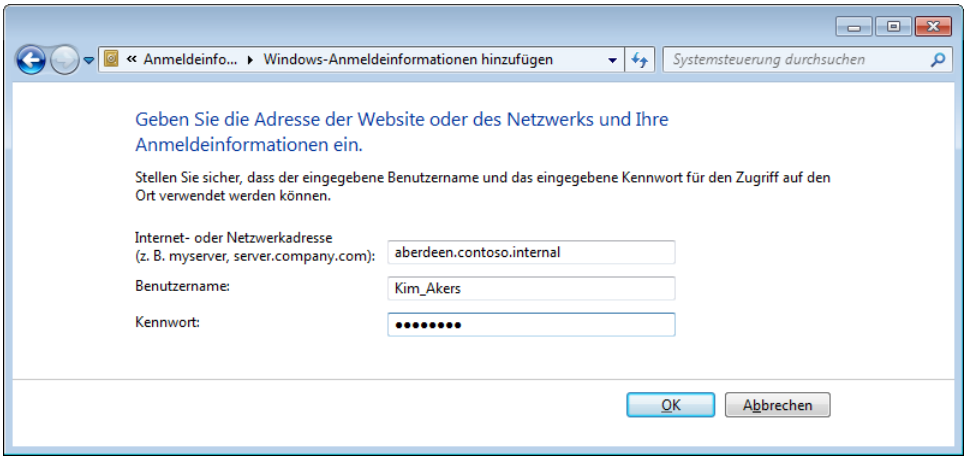

« Anmeldeinfo... ▸ Windows-Anmeldeinformationen hinzufügen
Systemsteuerung durchsuchen
Geben Sie die Adresse der Website oder des Netzwerks und Ihre Anmeldeinformationen ein.
Stellen Sie sicher, dass der eingegebene Benutzername und das eingegebene Kennwort für den Zugriff auf den Ort verwendet werden können.
Internet- oder Netzwerkadresse (z. B. myserver, server.company.com):
aberdeen.contoso.internal
Benutzername:
Kim_Akers
Kennwort:
••••••••
OK
Abbrechen

Abbildung 9.12 Hinzufügen von Windows-Anmeldeinformationen

Um ein Kennwort zu ändern oder Anmeldeinformationen zu löschen, klicken Sie den betreffenden Datensatz in der Anmeldeinformationsverwaltung an und dann das Element *Bearbeiten* oder *Aus Tresor entfernen*. Sie sehen diese Elemente in Abbildung 9.13. Nach einem Klick auf *Bearbeiten* können Sie den im Tresor gespeicherten Benutzernamen und das Kennwort ändern. Auf diese Weise lässt sich zum Beispiel ein gespeichertes Kennwort aktualisieren. Das vorhandene Kennwort wird nicht im Klartext angezeigt, sondern als eine

Folge von Punkten. Mit der Anmeldeinformationsverwaltung können Sie das gespeicherte Kennwort nicht ermitteln, sondern nur feststellen, dass ein Kennwort gespeichert wurde.

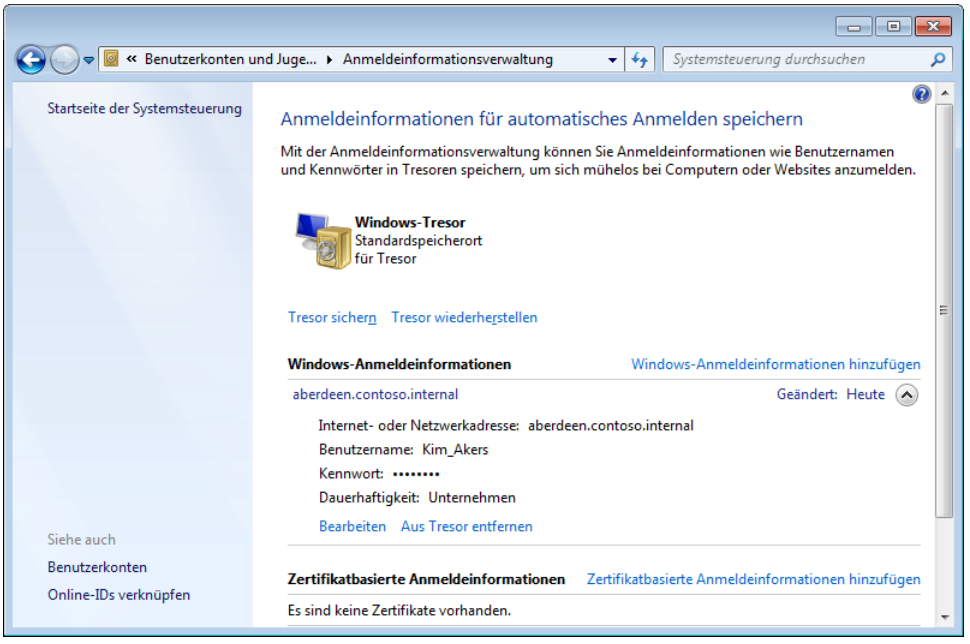


Abbildung 9.13 Bearbeiten und Entfernen von Anmeldeinformationen

Mit den Elementen *Tresor sichern* und *Tresor wiederherstellen*, die auch in Abbildung 9.13 zu sehen sind, können Sie Anmeldeinformationen sichern und auf demselben oder auf anderen Computern wiederherstellen. Auf diese Weise lassen sich Anmeldeinformationen auf andere Computer übertragen. Das kann sich als nützlich erweisen, wenn Benutzer auf ihren Windows 7-Computern viele Anmeldeinformationen gespeichert haben und diese nach einem Wechsel auf einen anderen Computer nicht alle neu eingeben möchten. Während der Sicherung müssen Sie die Tasten STRG+ALT+ENTF gleichzeitig drücken, damit ein Wechsel zum sicheren Desktop erfolgt, wo Sie das Kennwort zum Schutz der gesicherten Anmeldeinformationen eingeben. Außerdem müssen Sie bei der Wiederherstellung des Windows-Tresors die Tasten STRG+ALT+ENTF gleichzeitig drücken, um das Kennwort für die gesicherten Anmeldeinformationen auf dem sicheren Desktop eingeben zu können. In einer Übung am Ende dieser Lektion sichern Sie den Windows-Tresor und stellen ihn wieder her.

Ausführen von Programmen als anderer Benutzer mit Runas

Das Befehlszeilenprogramm Runas ermöglicht die Ausführung eines Programms mit den Anmeldeinformationen eines anderen Benutzers. Um eine Anwendung namens *Anwendung.exe* mit einer Option auszuführen, geben Sie die Anwendung und die Option in Anführungszeichen an. Wollen Sie zum Beispiel das Programm `Anwendung.exe /Option` auf dem Computer *Canberra* als Benutzer *Kim_Akers* ausführen, verwenden Sie folgenden Befehl:

```
Runas /user:Canberra\Kim_Akers "Anwendung.exe /Option"
```

Wenn Sie diesen Befehl verwenden, müssen Sie das Kennwort des verwendeten Kontos eingeben. Anschließend wird die Anwendung im Sicherheitskontext des angegebenen Zielbenutzers ausgeführt. Standardmäßig wird das Profil des Zielbenutzers geladen. Sie können auch mit der Option `/profile` explizit angeben, dass das Profil des Zielbenutzers geladen werden soll. Wenn das Profil des Zielbenutzers geladen ist, können Sie auf Dateien zugreifen, die mit dem Konto des Zielbenutzers verschlüsselt wurden, weil die EFS-Zertifikate in den Benutzerprofildaten gespeichert werden. Wenn das Profil nicht geladen werden soll, geben Sie die Option `/noprofile` an.

Die Option `/savecred` bewirkt die Speicherung der Anmeldeinformationen des Zielbenutzerkontos. Bei der ersten Verwendung der Option `/savecred` müssen Sie das Kennwort noch angeben. Bei allen weiteren Runas-Aufrufen, die mit diesen Anmeldeinformationen erfolgen sollen, geben Sie die Option `/savecred` und den Kontennamen an. Gespeicherte Anmeldeinformationen werden im Windows-Tresor gespeichert und können mit der Anmeldeinformationsverwaltung verwaltet werden. Der folgende Befehl ist ein Beispiel für die Verwendung von Runas mit der Option `/savecred`:

```
Runas /savecred /user:ComputerName\BenutzerName "Anwendung.exe /Option"
```

Mit dem Runas-Befehl können Sie keine Anwendung ausführen, die eine Erhöhung der Rechte erfordert, wenn das Zielkonto die Eingabe einer Zustimmung oder von Anmeldeinformationen erfordert. Sie können aber mit dem Runas-Befehl eine Anwendung ausführen, die eine Erhöhung der Rechte erfordert, wenn Sie das vordefinierte *Administrator*-Konto als Zielkonto verwenden. Standardmäßig ist das vordefinierte *Administrator*-Konto zwar deaktiviert, aber es kann in den Gruppenrichtlinien aktiviert werden. Nach der Aktivierung des *Administrator*-Kontos können Sie zum Beispiel als Standardbenutzer mit folgendem Befehl die Konsole *Editor für lokale Gruppenrichtlinien* starten:

```
runas /user:administrator "mmc gpedit.msc"
```

Auch die Anmeldeinformationen des lokalen Administratorkontos können Sie für eine künftige automatische Verwendung speichern, indem Sie zusätzlich die Option `/savecred` angeben. Seien Sie aber vorsichtig, wenn Sie dies tun, weil es ein Sicherheitsrisiko darstellt.

Konfigurieren von Benutzerrechten

Unter dem Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten* können Sie in den Gruppenrichtlinien Benutzerrechte konfigurieren. Dieser Knoten enthält 44 Richtlinien, von denen die meisten für Betriebssystemfunktionen vorgesehen sind, die in der Prüfung 70-680 wahrscheinlich nicht abgefragt werden. Die meisten Administratoren konfigurieren Benutzerrechte nicht durch eine Änderung bestimmter Gruppenrichtlinien, sondern indem sie Benutzer zu bestimmten lokalen Gruppen hinzufügen. Beispielsweise können Sie einem Benutzer erlauben, Dateien und Verzeichnisse zu sichern, indem Sie ihn zur Gruppe *Sicherungs-Operatoren* hinzufügen, statt die Richtlinie *Sichern von Dateien und Verzeichnissen* zu ändern. Das Gleiche gilt für die Verwendung von Remotedesktop. Sie können ein Benutzerkonto zur Gruppe *Remotedesktopbenutzer* hinzufügen oder Sie können die Richtlinie *Anmelden über Remotedesktopdienste zulassen* ändern. Gewöhnlich ist es einfacher, Mitglieder zu den entsprechenden lokalen Gruppen hinzuzufügen, weil sich anhand der Gruppenmitgliedschaft leichter überprüfen lässt, welchen Benutzern bestimmte Rechte zugewiesen wurden, als über die

Gruppenrichtlinieneinstellungen. Unter Windows 7 können Sie Benutzer folgenden vordefinierten Gruppen zuweisen, um ihnen Berechtigungen zuzuweisen:

- **Administratoren** Mitglieder dieser Gruppe haben unbeschränkten Zugriff auf den Windows 7-Computer.
- **Sicherungs-Operatoren** Mitglieder dieser Gruppe können Zugangsbeschränkungen für Dateien und Ordner außer Kraft setzen, um Daten zu sichern.
- **Kryptografie-Operatoren** Mitglieder dieser Gruppe können kryptografische Vorgänge durchführen. Diese Richtlinie wird nur verwendet, wenn Windows 7 in einer speziellen Konfiguration bereitgestellt wird, die Common Criteria Mode genannt wird. In diesem Modus können Administratoren alle Einstellungen lesen und schreiben, mit Ausnahme der Einstellungen für die Kryptografie in der IPsec-Richtlinie.
- **Distributed COM-Benutzer** Mitglieder dieser Gruppe können Distributed COM-Objekte auf diesem Computer bearbeiten.
- **Ereignisprotokollleser** Mitglieder dieser Gruppe können die Ereignisprotokolle lesen.
- **Netzwerkkonfigurations-Operatoren** Mitglieder dieser Gruppe können die Adresseinstellungen für TCP/IP (Transmission Control Protocol/Internet Protocol) ändern.
- **Leistungsprotokollbenutzer** Diese Benutzer können die Protokollierung von Leistungsindikatoren in die Aufgabenplanung eintragen, Ablaufverfolgungsanbieter aktivieren und Ereignisüberwachungsdaten sammeln.
- **Leistungsüberwachungsbenutzer** Diese Benutzer können Leistungsindikatoren lokal und remote verwenden.
- **Hauptbenutzer** Diese Gruppe gibt es noch aus Gründen der Abwärtskompatibilität.
- **Remotedesktopbenutzer** Mitglieder dieser Gruppe können sich über Remotedesktop remote anmelden.
- **Replikations-Operator** Diese Gruppe ist für Aufgaben aus dem Bereich der Datei-replikation in Domänenumgebungen vorgesehen.



Weitere Informationen Lokale Standardgruppen

Über lokale Standardgruppen erfahren Sie auf folgender Microsoft TechNet-Website mehr: *http://technet.microsoft.com/de-de/library/cc771990.aspx*. Berücksichtigen Sie aber, dass einige der beschriebenen Gruppen nur in Domänenumgebungen wichtig sind.

Schnelltest

- Wie können Sie Anmeldeinformationen löschen, die Sie bei der Verwendung von Runas mit der Option `/savecred` gespeichert haben?

Antwort zum Schnelltest

- Sie können die Anmeldeinformationen in der Anmeldeinformationsverwaltung löschen.

Smartcards

Smartcards speichern digitale Zertifikate, die sich für eine Authentifizierung eignen. Smartcards sind sicherer als eine Authentifizierung mit Benutzernamen und Kennwort. Jemand könnte sich zwar den Benutzernamen und das Kennwort eines anderen Benutzers verschaffen und verwenden, ohne dass der andere Benutzer darauf aufmerksam wird, aber es ist sehr schwierig für jemanden, sich eine Smartcard zu verschaffen, ohne dass dies dem Eigentümer der Smartcard nicht nach einer gewissen Zeit auffällt. Wird eine Smartcard vermisst, kann ein Administrator das auf der Smartcard gespeicherte Zertifikat sperren. Dadurch wird die Smartcard für eine Authentifizierung unbrauchbar.

Windows 7 unterstützt den PIV-Standard des National Institute of Standards and Technology (NIST). Dadurch wird es möglich, Treiber für Smartcards von Windows Update zu erhalten oder einen PIV-konformen Minitreiber von Windows 7 zu verwenden. Das hat den Vorteil, dass Sie Smartcards ohne herstellerspezifische Software mit Windows 7 verwenden können.

Smartcards ermöglichen eine mehrstufige Authentifizierung auf Windows 7-Computern. *Mehrstufige Authentifizierung* bedeutet, dass ein Benutzer zur Authentifizierung zwei oder mehr separate Komponenten benötigt. Der Benutzer muss vielleicht einen Benutzernamen und ein Kennwort eingeben und zusätzlich eine Smartcard in das Lesegerät einlegen, oder er führt die Authentifizierung mit Benutzernamen, Kennwort und einer biometrischen Methode durch, beispielsweise mit einem Fingerabdruck. Die gebräuchlichste Form der mehrstufigen Authentifizierung unter Windows 7 ist in Unternehmensumgebungen die Authentifizierung mit Smartcard und Kennwort. Eine biometrische Authentifizierung wird eher auf portablen eigenständigen Windows 7-Computern verwendet und lässt sich nicht ohne zusätzliche Software in die Active Directory-Domänendienste integrieren.



Weitere Informationen Biometrie in Windows 7

Eine biometrische Authentifizierung wird wahrscheinlich nicht Thema der Prüfung 70-680 sein, aber Sie können auf der folgenden Microsoft TechNet-Webseite mehr über dieses Thema erfahren: *http://technet.microsoft.com/de-de/library/dd367857.aspx.*

Unter Windows 7 gibt es im Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen* einige Richtlinien für Smartcards:

- **Interaktive Anmeldung: Smartcard erforderlich** Wird diese Richtlinie aktiviert, können sich Benutzer nur noch mit einer Smartcard am Computer anmelden. Wenn diese Richtlinie deaktiviert ist (Standardeinstellung), können sich Benutzer mit allen anderen zulässigen Methoden anmelden.
- **Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards** Mit dieser Richtlinie können Sie festlegen, wie sich der Computer verhalten soll, wenn ein Benutzer seine Smartcard aus dem Lesegerät entfernt. Die Standardeinstellung ist, bei der Entfernung der Smartcard nichts zu tun. Die anderen verfügbaren Einstellungen sind:
  - **Arbeitsstation sperren** Wenn Sie diese Einstellung vornehmen, sperrt Windows 7 die Arbeitsstation, wenn die Smartcard entfernt wird. Der Benutzer kann die Sperrung nur aufheben, indem er die Smartcard wieder in das Lesegerät einlegt.

- **Abmeldung erzwingen** Wenn Sie diese Einstellung vornehmen, wird der Benutzer automatisch abgemeldet, sobald seine Smartcard entfernt wird.
- **Trennen, falls Remotedesktopdienste-Sitzung** Diese Richtlinie gilt für Terminaldienstesitzungen, die unter Windows Server 2008 abgehalten werden. Unter Windows Server 2008 R2 wurden die Terminaldienste in Remotedesktopdienste umbenannt. Der Benutzer wird automatisch von der Remotedesktopdienstesitzung getrennt, wenn seine Smartcard aus dem Lesegerät entfernt wird.



Weitere Informationen Smartcards in Windows 7

Weitere Informationen über die Verwendung von Smartcards unter Windows 7 finden Sie auf der folgenden Microsoft TechNet-Webseite: *http://technet.microsoft.com/de-de/library/dd367851.aspx*.

Kontorichtlinien

Mit den Kennwort- und Kontosperrungsrichtlinien, die in den Gruppenrichtlinien unter *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen* zu finden sind, können Sie Einstellungen für Kennwörter und Kontosperrungen vornehmen. Sie können zum Beispiel festlegen, wie lange ein Benutzer ein Kennwort verwenden darf, bevor er es ändern muss, ob ein Konto nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen gesperrt wird und ob Kennwörter bestimmte Komplexitätsanforderungen erfüllen müssen.

Sie können folgende Kennwortrichtlinien verwenden:

- **Kennwortchronik erzwingen** Mit dieser Richtlinie erreichen Sie, dass die Leute nicht nur eine geringe Anzahl von Kennwörtern benutzen, die sie bei jeder geforderten Kennwortänderung immer wieder abwechselnd verwenden. Wenn Sie die Richtlinie *Kennwortchronik erzwingen* konfigurieren, speichert Windows 7 eine gewisse Anzahl der veralteten Kennwörter und lässt nicht zu, dass die Benutzer als neues Kennwort ein Kennwort einstellen, dass sie bereits verwendet haben. Bei der Konfiguration dieser Richtlinie legen Sie fest, wie viele Kennwörter gespeichert werden.
- **Maximales Kennwortalter** Der Zeitraum (in Tagen), für den ein Benutzer dasselbe Kennwort verwenden kann. Nach Ablauf dieses Zeitraums muss der Benutzer sein Kennwort ändern. Wurde für ein Benutzerkonto die Einstellung *Kennwort läuft nie ab* vorgenommen (nicht empfohlen), gilt diese Richtlinie nicht für dieses Konto.
- **Minimales Kennwortalter** Mit dieser Richtlinie legen Sie den Zeitraum (in Tagen) fest, in dem ein Kennwort nicht geändert werden kann. Das hindert Benutzer daran, ihre Kennwörter einige Male hintereinander zu ändern, bis sie wieder das alte Kennwort verwenden können, das sie vor der Aufforderung zur Kennwortänderung verwendet hatten.
- **Minimale Kennwortlänge** Mit dieser Richtlinie legen Sie fest, aus wie vielen Zeichen ein Kennwort mindestens bestehen muss.
- **Kennwort muss Komplexitätsvoraussetzungen entsprechen** Wenn diese Richtlinie aktiviert ist, müssen Kennwörter Zeichen aus mindestens drei der folgenden Gruppen enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern und Symbole. Außerdem dürfen Kennwörter dann nicht den Kontonamen des Benutzers oder Teile seines Vor- oder Nachnamens enthalten.

- **Kennwörter mit umkehrbarer Verschlüsselung speichern** Verwenden Sie diese Richtlinie nur, wenn Sie ältere Anwendungen einsetzen, die ältere Authentifizierungsmethoden verwenden. Durch diese Richtlinie ist die Speicherung von Kennwörtern weniger sicher.

Sie können die folgenden Kontosperrungsrichtlinien konfigurieren:

- **Kontosperrdauer** Mit dieser Richtlinie legen Sie fest, wie lange ein gesperrtes Konto gesperrt bleibt, bis sich ein Benutzer wieder anmelden kann.
- **Kontensperrungsschwelle** Mit dieser Richtlinie legen Sie fest, wie oft ein Benutzer ein falsches Kennwort eingeben kann, bevor Windows das Konto sperrt.
- **Zurücksetzungsdauer des Kontosperrungszählers** Mit dieser Richtlinie legen Sie den Zeitraum fest, in dem Windows ungültige Anmeldeversuche mitzählt. Wenn Sie diesen Zeitraum beispielsweise auf 30 Minuten einstellen und die Richtline *Kontensperrungsschwelle* auf 3 eingestellt ist, lösen 3 ungültige Anmeldeversuche in 30 Minuten eine Sperrung aus, während 3 ungültige Anmeldeversuche in 31 Minuten dies nicht tun. Eine gültige Anmeldung setzt den Zähler für nicht erfolgreiche Anmeldeversuche zurück.

Beheben von Authentifizierungsproblemen

Das häufigste Authentifizierungsproblem, mit dem es Benutzer zu tun haben, ist ein vergessenes Kennwort. Es gibt zwei Methoden zur Behebung dieses Problems: Kennwortrücksetzdatenträger und das Zurücksetzen des Kennworts des Benutzerkontos. Kennwortrücksetzdatenträger, zu denen auch USB-Speichergeräte (Universal Serial Bus) gehören können, haben den Vorteil, dass sie den Zugang zum Computer ermöglichen, ohne dass verschlüsselte Daten verloren gehen. Ihr Nachteil besteht darin, dass man einen Kennwortrücksetzdatenträger erstellen muss, bevor das Kennwort verloren geht. Ein weiterer Nachteil besteht darin, dass jeder, der im Besitz dieses Datenträgers ist, für das betreffende Konto ein neues Kennwort festlegen kann. Daher müssen die Datenträger sicher verwahrt werden, denn jeder, der Zugriff auf einen Kennwortrücksetzdatenträger hat, kann sich Zugang zum Computer des Benutzers verschaffen.

Um einen Kennwortrücksetzdatenträger zu erstellen, wobei es sich um eine Diskette oder um ein USB-Flashlaufwerk handeln kann, verwenden Sie auf der Seite *Benutzerkonten* der Systemsteuerung das Element *Kennwortrücksetzdiskette erstellen*. Ein Klick auf das Element *Kennwortrücksetzdiskette erstellen* startet den Assistenten für vergessene Kennwörter. Im Assistenten wählen Sie den Wechseldatenträger aus, auf dem Sie die Daten speichern möchten, und geben dann das aktuelle Kennwort des Benutzerkontos ein (Abbildung 9.14). Sie können den Kennwortrücksetz-Assistenten aktivieren, nachdem auf dem Anmeldebildschirm von Windows 7 ein falsches Kennwort eingegeben wurde. Wenn ein Benutzer diesen Assistenten verwendet, wählt er das Laufwerk aus, auf dem sich die Kennwortrücksetzdaten befinden (Diskette oder USB-Gerät), und gibt dann ein neues Kennwort ein. Anschließend erhält er wieder Zugang zum Computer und zu allen seinen verschlüsselten Daten.

Wenn ein Benutzer sein Kennwort vergessen hat und kein Kennwortrücksetzdatenträger verfügbar ist, muss das Kennwort geändert werden. Das kann über den Knoten *Benutzer* der Konsole *Computerverwaltung* oder unter Verwendung der Option *Anderes Konto verwalten* auf der Seite *Benutzerkonten* der Systemsteuerung erfolgen. Nur Mitglieder der lokalen Gruppe *Administratoren* können das Kennwort eines anderen Benutzers ändern. Wenn Sie

das Kennwort eines Benutzers ändern, verliert der Benutzer den Zugriff auf seine EFS-verschlüsselten Dateien, auf seine persönlichen Zertifikate und auf die gespeicherten Kennwörter, die im Windows-Tresor gespeichert wurden (Abbildung 9.15).

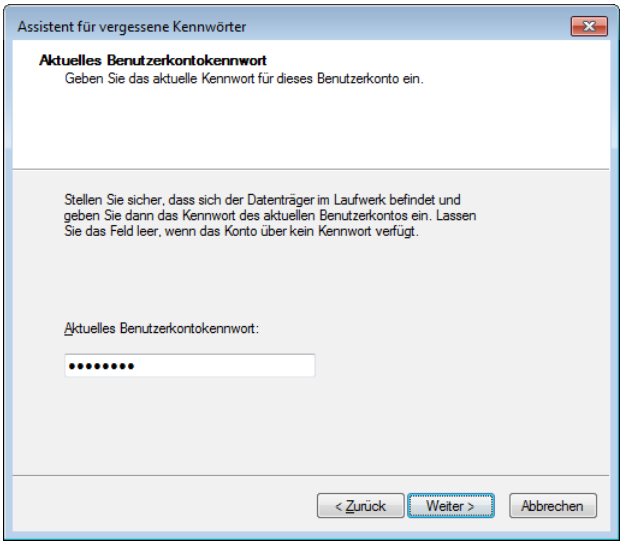

Assistent für vergessene Kennwörter
Aktuelles Benutzerkontokennwort
Geben Sie das aktuelle Kennwort für dieses Benutzerkonto ein.
Stellen Sie sicher, dass sich der Datenträger im Laufwerk befindet und geben Sie dann das Kennwort des aktuellen Benutzerkontos ein. Lassen Sie das Feld leer, wenn das Konto über kein Kennwort verfügt.
Aktuelles Benutzerkontokennwort:
••••••••
< Zurück
Weiter >
Abbrechen

Abbildung 9.14 Erstellen eines Kennwortrücksetzdatenträgers

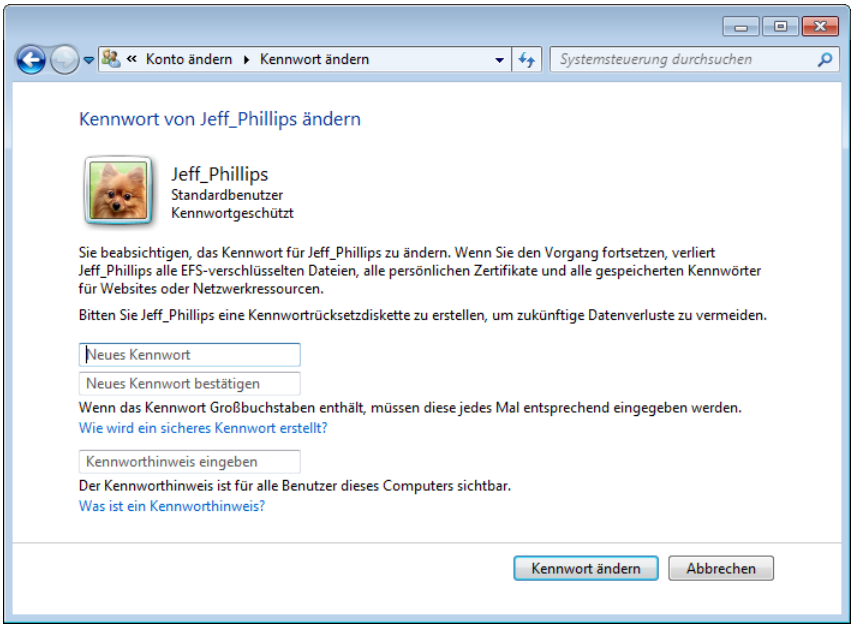

« Konto ändern ▸ Kennwort ändern
Systemsteuerung durchsuchen
Kennwort von Jeff_Phillips ändern
Jeff_Phillips
Standardbenutzer
Kennwortgeschützt
Sie beabsichtigen, das Kennwort für Jeff_Phillips zu ändern. Wenn Sie den Vorgang fortsetzen, verliert Jeff_Phillips alle EFS-verschlüsselten Dateien, alle persönlichen Zertifikate und alle gespeicherten Kennwörter für Websites oder Netzwerkressourcen.
Bitten Sie Jeff_Phillips eine Kennwortrücksetzdiskette zu erstellen, um zukünftige Datenverluste zu vermeiden.
Neues Kennwort
Neues Kennwort bestätigen
Wenn das Kennwort Großbuchstaben enthält, müssen diese jedes Mal entsprechend eingegeben werden.
Wie wird ein sicheres Kennwort erstellt?
Kennworthinweis eingeben
Der Kennworthinweis ist für alle Benutzer dieses Computers sichtbar.
Was ist ein Kennworthinweis?
Kennwort ändern
Abbrechen

Abbildung 9.15 Eine Änderung des Kennworts anderer Benutzer ist mit einigen Nachteilen verbunden

Sofern der Benutzer diese Kennwörter und Zertifikate gesichert hat, ist es vielleicht möglich, den Windows-Tresor wiederherzustellen. Hat der Benutzer seinen EFS-Schlüssel gesichert, kann er wieder auf die verschlüsselten Dateien zugreifen, wenn er diesen Schlüssel wiederherstellt. Im Verlauf dieser Lektion wird die Sicherung und Wiederherstellung von EFS-Schlüsseln noch besprochen. Außerdem kann ein Administrator EFS-verschlüsselte Dateien wiederherstellen, wenn auf dem Computer ein EFS-Wiederherstellungsagent konfiguriert wurde. Die Erstellung eines EFS-Wiederherstellungsagenten wird in Kapitel 8, »BranchCache und Ressourcenfreigabe«, beschrieben.

Falls Sie Kontosperrungsrichtlinien konfiguriert haben, hat sich der Benutzer vielleicht ausgesperrt, weil er die in den Richtlinien festgelegte Zahl der unzulässigen Anmeldeversuche erreicht hat. Um die Sperrung des Kontos aufzuheben, können Sie in der Konsole *Computerverwaltung* das Kontrollkästchen neben *Konto ist gesperrt* löschen (Abbildung 9.16). Nur Mitglieder der lokalen Gruppe *Administratoren* können die Sperrung eines Kontos aufheben. Die Aufhebung der Sperrung setzt das Kennwort nicht zurück und wirkt sich nicht auf gespeicherte Anmeldeinformationen oder EFS-Zertifikate aus. Ein Benutzer, dessen Konto gesperrt wurde, muss das Kennwort noch kennen, um sich am Computer anmelden zu können.

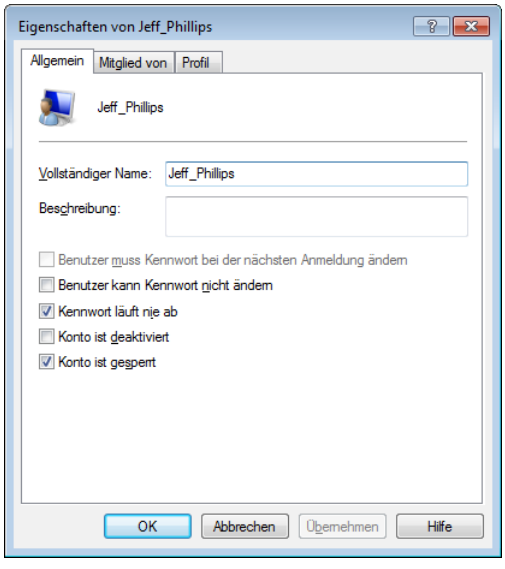


Abbildung 9.16 Das Konto ist gesperrt

Verwalten von Zertifikaten

EFS-Zertifikate lassen sich zwar nicht mit der Anmeldeinformationsverwaltung sichern, aber Windows 7 bietet zu diesem Zweck drei andere Tools. Dabei handelt es sich um die *Zertifikate*-Konsole (*Certmgr.msc*), das Tool *Dateiverschlüsselungszertifikate verwalten* und das Befehlszeilentool *Cipher.exe*. Jedes dieser Tools lässt sich dazu verwenden, ein vorhandenes EFS-Zertifikat in eine kennwortgeschützte PFX-Datei zu exportieren oder zu sichern. Diese PFX-Datei kann dann auf anderen Computern importiert oder bei Bedarf auf dem ursprünglichen Computer zur Wiederherstellung verwendet werden. Dazu verwenden Sie

entweder eines dieser Tools oder klicken die PFX-Datei im Windows-Explorer mit einem Doppelklick an.

Die meisten Benutzer werden zur Sicherung ihrer EFS-Zertifikate das Tool *Dateiverschlüsselungszertifikate verwalten* verwenden, weil es leichter zu verwenden ist als die anderen Tools (Abbildung 9.17). Dieses Tool enthält einen Wizard, mit dem Sie Ihre Zertifikate sichern oder eine Smartcard für die Verwendung mit EFS einrichten können. Um das Tool zu öffnen, geben Sie im Textfeld *Programme/Dateien durchsuchen* **Dateiverschlüsselungszertifikate verwalten** ein. Im Assistenten können Sie das zu sichernde Zertifikat auswählen, einen Ort für die Speicherung der Sicherungsdatei festlegen und ein Kennwort für den Schutz der Sicherungsdatei angeben.

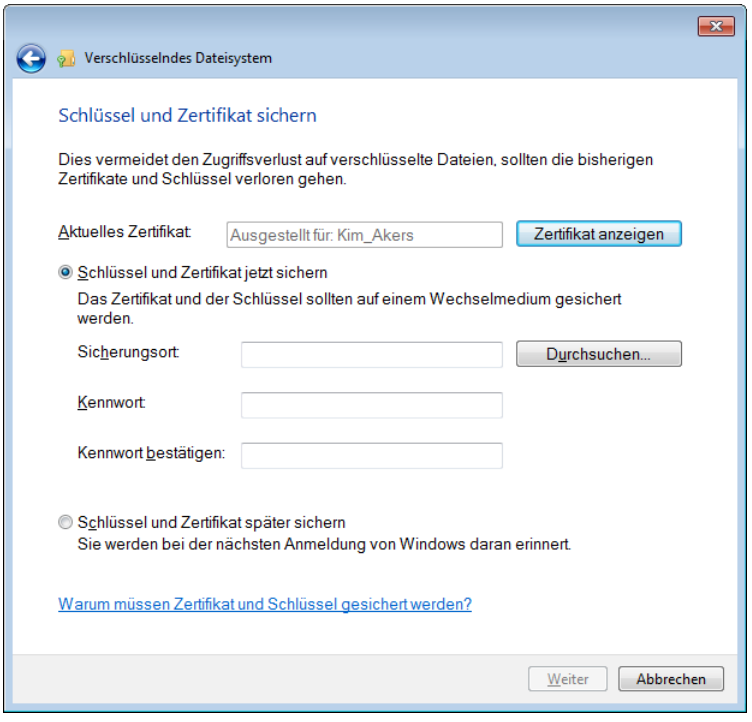

Verschlüsselndes Dateisystem
Schlüssel und Zertifikat sichern
Dies vermeidet den Zugriffsverlust auf verschlüsselte Dateien, sollten die bisherigen Zertifikate und Schlüssel verloren gehen.
Aktuelles Zertifikat:
Ausgestellt für: Kim_Akers
Zertifikat anzeigen
Schlüssel und Zertifikat jetzt sichern
Das Zertifikat und der Schlüssel sollten auf einem Wechselmedium gesichert werden.
Sicherungsort:
Durchsuchen...
Kennwort:
Kennwort bestätigen:
Schlüssel und Zertifikat später sichern
Sie werden bei der nächsten Anmeldung von Windows daran erinnert.
Warum müssen Zertifikat und Schlüssel gesichert werden?
Weiter
Abbrechen

Abbildung 9.17 Sichern des EFS-Zertifikats

Auch die *Zertifikate*-Konsole eignet sich zur Sicherung der EFS-Zertifikate (Abbildung 9.18). Diese Konsole lässt sich durch die Eingabe von **Certmgr.msc** ins Textfeld *Programme/Dateien durchsuchen* öffnen. Um ein Zertifikat in eine kennwortgeschützte PFX-Datei zu exportieren, klicken Sie es mit der rechten Maustaste an, wählen *Alle Aufgaben* und klicken dann auf *Exportieren*. Normale Benutzer werden diese Konsole wahrscheinlich nicht verwenden, weil sie komplizierter ist als das Tool *Dateiverschlüsselungszertifikate verwalten*. Sie müssen zum Beispiel wissen, dass Ihr EFS-Zertifikat unter dem Knoten *Eigene Zertifikate/Zertifikate* zu finden ist. Für einen Benutzer, der technisch nicht interessiert ist, dürfte das keinesfalls »intuitiv« sein.

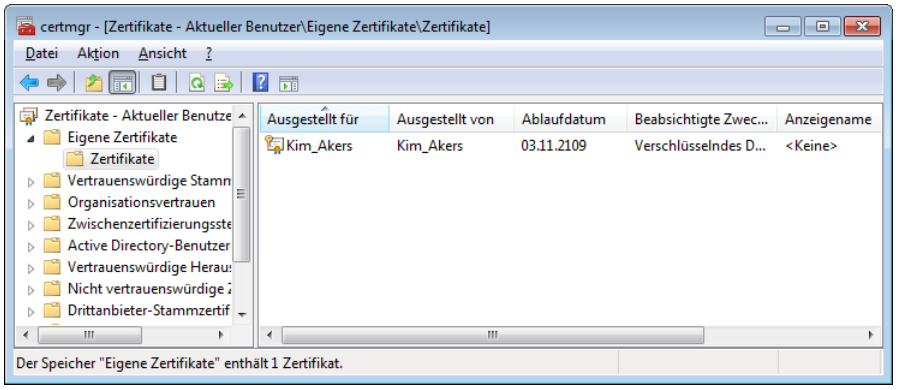


Abbildung 9.18 Die *Zertifikate*-Konsole (*Certmgr.msc*)

Mit dem Befehlszeilenprogramm *Cipher.exe* lassen sich EFS-Zertifikate auch auf der Befehlszeile sichern. Wenn Sie Ihren Schlüssel sichern, wird auf dem Desktop eine Warnmeldung angezeigt, die Sie auf den anstehenden Vorgang hinweist. Anschließend werden Sie aufgefordert, zum Schutz der PFX-Datei ein Kennwort einzugeben. Der Befehl zur Sicherung eines EFX-Zertifikats lautet:

```
cipher.exe /x Dateiname.pfx
```



Prüfungstipp

Merken Sie sich, welche Aufgaben Sie in der Anmeldeinformationsverwaltung durchführen können.

Übung Verwalten von Anmeldeinformationen

Der Windows-Tresor ermöglicht Ihnen die Speicherung von Anmeldeinformationen. Das ist sehr nützlich, wenn Sie außerhalb eines Domänennetzwerks auf Ressourcen zugreifen müssen und sich die Kennwörter und Anmeldenamen nicht merken können, die Sie für die verschiedenen Ressourcen brauchen. In dieser Übung untersuchen Sie den Windows-Tresor und das Tool Runas. Sie werden einen Eindruck davon bekommen, welche Aufgaben diese Komponenten haben und wie Sie diese Komponenten bei der Bereitstellung von Windows 7 in Ihrem eigenen Netzwerk verwenden.

Übung 1 Experimentieren mit Runas und der Anmeldeinformationsverwaltung

In dieser Übung verwenden Sie den Befehl Runas, um einige Anwendungen mit den Anmeldeinformationen eines anderen Benutzers auszuführen. Diese Anmeldeinformationen speichern Sie im Windows-Tresor, überprüfen, ob sie gespeichert wurden, und entfernen sie wieder:

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Anmeldeinformationsverwaltung** ein**.** Klicken Sie auf *Anmeldeinformationsverwaltung*. Überprüfen Sie, ob unter den verschiedenen Kategorien bereits Anmeldeinformationen gespeichert sind. Schließen Sie Anmeldeinformationsverwaltung.

3. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und verwenden Sie folgenden Befehl:

   ```
   Net user Dan_Park P@ssw0rd /ADD
   ```

4. Schließen Sie die Eingabeaufforderung mit erhöhten Rechten. Öffnen Sie eine normale Eingabeaufforderung und öffnen Sie den Editor mit folgendem Befehl:

   ```
   Runas /savecred /user:Canberra\Dan_Park notepad
   ```

5. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort **P@ssw0rd** ein. Schließen Sie den Editor. Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

   ```
   Runas /user:Canberra\Dan_Park write
   ```

6. Um WordPad zu starten, mussten Sie das Kennwort eingeben. Schließen Sie WordPad. Geben Sie in der Eingabeaufforderung folgenden Befehl ein, um Microsoft Paint zu öffnen:

   ```
   Runas /savecred /user:Canberra\Dan_Park mspaint
   ```

7. Diesmal brauchten Sie kein Kennwort einzugeben, weil die gespeicherten Anmeldeinformationen verwendet wurden. Schließen Sie Paint.

8. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Anmeldeinformationsverwaltung** ein. Klicken Sie auf *Anmeldeinformationsverwaltung*. Klicken Sie unter *Windows-Anmeldeinformationen* auf den Eintrag *Canberra\Dan_Park* (Abbildung 9.19).

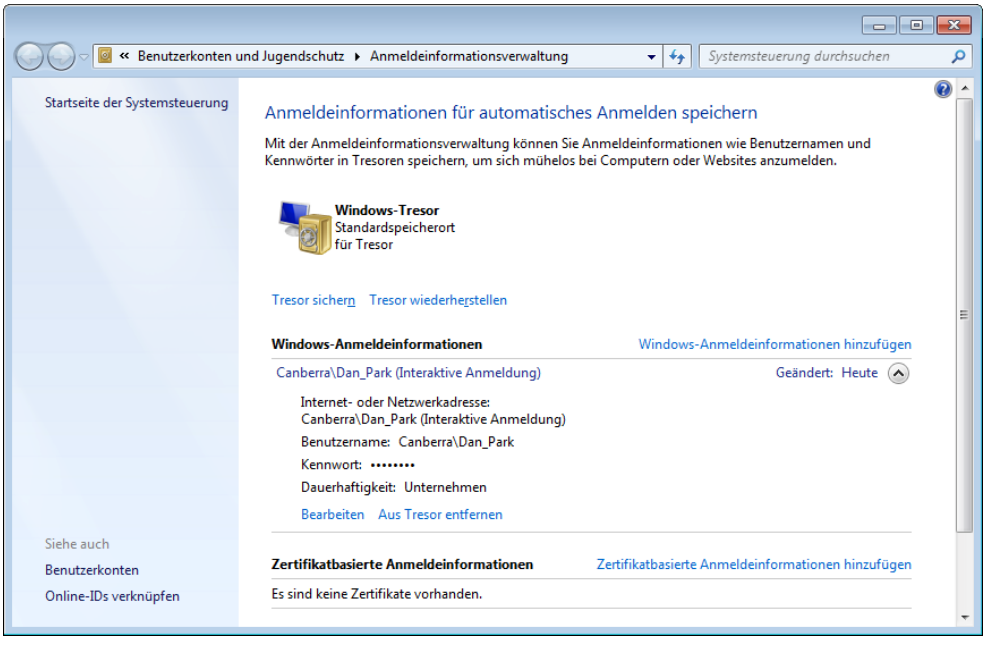


Abbildung 9.19 Gespeicherte Anmeldeinformationen

9. Klicken Sie auf *Aus Tresor entfernen*, um die Anmeldeinformationen von Dan Park zu entfernen. Klicken Sie im Dialogfeld *Windows-Anmeldeinformationen löschen* auf *Ja*. Verwenden Sie in der Eingabeaufforderung erneut folgenden Befehl:

   ```
   Runas /savecred /user:Canberra\Dan_Park mspaint
   ```

10. Diesmal müssen Sie das Kennwort eingeben, weil die Anmeldeinformationen nicht mehr im Windows-Tresor gespeichert waren (durch die Verwendung dieses Befehls wurden sie allerdings wieder hinzugefügt).

Übung 2 Hinzufügen von Anmeldeinformationen, Sichern und Wiederherstellen des Windows-Tresors

In dieser Übung fügen Sie die Anmeldeinformationen für ein weiteres Konto zu dem einen Datensatz hinzu, der in der vorigen Übung zum Windows-Tresor hinzugefügt wurde. Anschließend sichern Sie den Windows-Tresor, löschen die vorhandenen Anmeldeinformationen und stellen den Windows-Tresor wieder her.

1. Sofern Sie es noch nicht getan haben, melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an. Erstellen Sie im Windows-Explorer das Verzeichnis *C:\Tresor*.
2. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Anmeldeinformationsverwaltung** ein**.** Klicken Sie auf *Anmeldeinformationsverwaltung*.
3. Überprüfen Sie, ob der Eintrag *Canberra\Dan_Park (Interaktive Anmeldung)* noch in der Anmeldeinformationsverwaltung vorhanden ist. Diesen Datensatz haben Sie in Schritt 9 von Übung 1 erneut erstellt.
4. Klicken Sie auf *Windows-Anmeldeinformationen hinzufügen*. Geben Sie im Dialogfeld *Windows-Anmeldeinformationen hinzufügen* folgende Anmeldeinformationen ein:
   - *Internet- oder Netzwerkadresse*: **Aberdeen.contoso.internal**
   - *Benutzername*: **Sam_Abolrous**
   - *Kennwort*: **P@ssword**

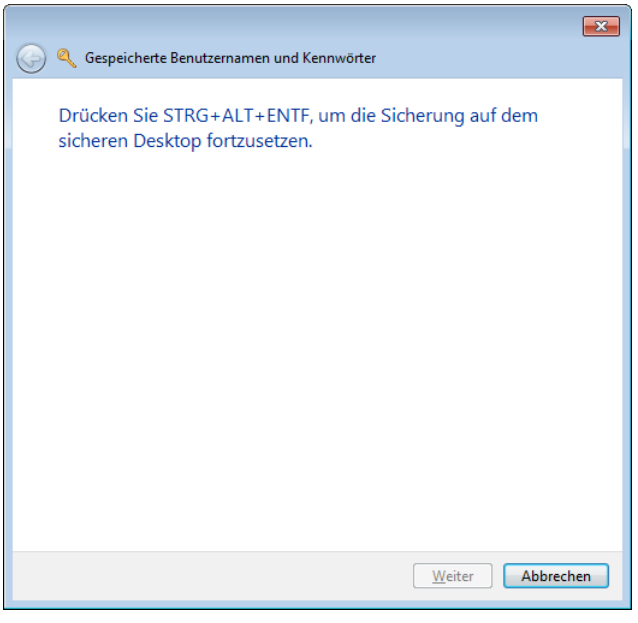

Gespeicherte Benutzernamen und Kennwörter
Drücken Sie STRG+ALT+ENTF, um die Sicherung auf dem sicheren Desktop fortzusetzen.
Weiter
Abbrechen

Abbildung 9.20 Datensicherung auf dem sicheren Desktop

5. Klicken Sie auf *OK*, um das Dialogfeld *Windows-Anmeldeinformationen hinzufügen* zu schließen.
6. Klicken Sie auf das Element *Tresor sichern*. Es öffnet sich das Dialogfeld *Gespeicherte Benutzernamen und Kennwörter*. Klicken Sie auf die Schaltfläche *Durchsuchen*. Wechseln Sie in den Ordner *C:\Tresor*, geben Sie den Namen **WinTresor** ein und klicken Sie auf *Speichern*. Klicken Sie auf *Weiter*.
7. Drücken Sie gleichzeitig auf die Tasten STRG+ALT+ENTF, um die Sicherung auf dem sicheren Desktop fortzusetzen (Abbildung 9.20).
8. Geben Sie zweimal das Kennwort **P@ssw0rd** ein und klicken Sie dann auf *Weiter*. Klicken Sie auf *Fertig stellen*.
9. Entfernen Sie in der Anmeldeinformationsverwaltung die Einträge *Aberdeen.contoso.internal* und *Canberra\Dan_Park (Interaktive Anmeldung)*.
10. Klicken Sie auf das Element *Tresor wiederherstellen*.
11. Klicken Sie auf *Durchsuchen*, suchen Sie die Datei *C:\Tresor\WinTresor.crd* heraus und klicken Sie dann auf *Weiter*.
12. Drücken Sie gleichzeitig auf die Tasten STRG+ALT+ENTF, um die Wiederherstellung der Anmeldeinformationen auf dem sicheren Desktop fortzusetzen.
13. Geben Sie im Dialogfeld *Gespeicherte Benutzernamen und Kennwörter* das Kennwort **P@ssw0rd** ein (Abbildung 9.21) und klicken Sie dann auf *Weiter*.

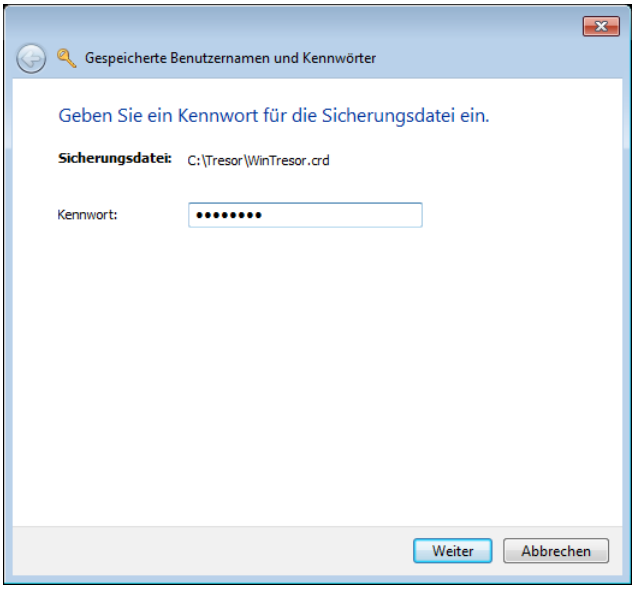


Abbildung 9.21 Wiederherstellen der Anmeldeinformationen

14. Wenn die Anmeldeinformationen wiederhergestellt sind, klicken Sie auf *Fertig stellen*.
15. Schließen Sie die Anmeldeinformationsverwaltung und öffnen Sie sie erneut, um zu überprüfen, ob die gelöschten Anmeldeinformationen wiederhergestellt wurden.

Zusammenfassung der Lektion

- Die Anmeldeinformationsverwaltung ermöglicht die Verwaltung von Kennwörtern für Websites, Terminaldienste und Remotedesktopsitzungen, einzelne Netzwerkressourcen und Smartcard-Zertifikate. Sie können die Anmeldeinformationsverwaltung verwenden, um diese Anmeldeinformationen zu sichern und wiederherzustellen.
- Das Tool Runas ermöglicht die Ausführung von Programmen mit den Anmeldeinformationen anderer Benutzer. Durch die zusätzliche Angabe der Option `/savecred` können Sie die Anmeldeinformationen speichern.
- Zur Sicherung von EFS-Zertifikaten können Sie *Certmgr.msc*, *Cipher.exe* oder das Tool *Dateiverschlüsselungszertifikate verwalten* verwenden.
- Benutzer können für den Fall, dass sie ihr Kennwort vergessen, Kennwortrücksetzdisketten erstellen. Allerdings muss der Kennwortrücksetzdatenträger erstellt werden, bevor dies geschieht.
- Mitglieder der lokalen Gruppe *Administratoren* können die Kennwörter von Benutzern zurücksetzen, die ihre Kennwörter vergessen haben.
- In den Gruppenrichtlinien lässt sich eine mehrstufige Authentifizierung konfigurieren, wobei sich Benutzer mit Smartcards anmelden müssen.
- Sie können Benutzern Rechte zuweisen, indem Sie sie zu einer passenden vordefinierten Gruppe hinzufügen oder die Rechte in den Gruppenrichtlinien zuweisen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 2, »Windows 7-Authentifizierung und -autorisierung«, überprüfen. Die Fragen sind (in englischer Sprache) auch auf der Begleit-CD zu finden, falls Sie die elektronische Form der Fragen vorziehen.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie haben auf einem Windows 7-Computer Runas mit der Option `/savecred` verwendet, um die Anmeldeinformationen eines Administratorkontos zu speichern. Die geplanten Aufgaben sind erledigt, und nun wollen Sie diese Anmeldeinformationen wieder löschen. Mit welchem der folgenden Tools können Sie dies tun?
   A. Runas
   B. Anmeldeinformationsverwaltung
   C. *Zertifikate*-Konsole
   D. Einstellungen der Benutzerkontensteuerung
2. Sie möchten sicherstellen, dass Benutzer automatisch von ihren Windows 7-Computern abgemeldet werden, wenn sie ihre Smartcards entfernen. Mit welchen der folgenden Richtlinien und Einstellungen erreichen Sie dies? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)

   A. *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards: Keine Aktion*
   B. *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards: Arbeitsstation sperren*
   C. *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards: Abmeldung erzwingen*
   D. *Interaktive Anmeldung: Smartcard erforderlich: Aktiviert*

3. Ein Benutzer hat das Kennwort für einen eigenständigen Windows 7-Computer vergessen, den er in Ihrer Organisation benutzt. Er hat keine Kennwortrücksetzdiskette. Sie haben auf diesem Computer ein Konto, das Mitglied der lokalen Gruppe *Administratoren* ist. Wie können Sie das Authentifizierungsproblem beheben?
   A. Sie heben die Sperrung des Kontos auf.
   B. Sie setzen das Kennwort zurück.
   C. Sie erstellen für das Konto des Benutzers eine Kennwortrücksetzdiskette.
   D. Sie erstellen für Ihr eigenes Konto eine Kennwortrücksetzdiskette.
4. Sie möchten sicherstellen, dass die Benutzer der eigenständigen Windows 7-Computer in Ihrer Organisation alle 3 Wochen ihre Kennwörter ändern. Welche der folgenden Richtlinien sollten Sie auf jedem Computer konfigurieren?
   A. *Kennwortchronik erzwingen*
   B. *Minimale Kennwortlänge*
   C. *Minimales Kennwortalter*
   D. *Maximales Kennwortalter*
5. Mit welchen der folgenden Tools können Benutzer ihre EFS-Zertifikate sichern, die erstellt wurden, als sie zum ersten Mal auf einem eigenständigen Windows 7-Computer eine Datei verschlüsselt haben? (Wählen Sie alle zutreffenden Antworten.)
   A. Anmeldeinformationsverwaltung
   B. Tool *Dateiverschlüsselungszertifikate verwalten*
   C. Konsole *Zertifikate*
   D. *Cipher.exe*

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Die Benutzerkontensteuerung kann für eine Eingabeaufforderung zu Anmeldeinformationen oder eine Eingabeaufforderung zur Zustimmung konfiguriert werden. Bei der Eingabeaufforderung zu Anmeldeinformationen müssen Sie Ihr Benutzerkonto und Ihr Kennwort angeben.
- Wenn ein Wechsel zum sicheren Desktop erfolgt, müssen Benutzer auf die Eingabeaufforderung der Benutzerkontensteuerung reagieren, bevor sie wieder am Computer arbeiten können.
- Die Benutzerkontensteuerung wird in den Gruppenrichtlinien konfiguriert.
- Die Anmeldeinformationsverwaltung speichert Anmeldeinformationen, die im Internet Explorer, für Remotedesktopverbindung und im Windows-Explorer bei Verbindungen mit Remoteservern eingegeben werden. Sie können diese Anmeldeinformationen sichern und wiederherstellen.
- Kennwortrichtlinien legen fest, in welchen Zeitabständen ein Kennwort geändert werden muss, ob das Benutzerkonto nach der Eingabe einer bestimmten Anzahl von falschen Kennwörtern gesperrt wird und wie komplex Kennwörter sein müssen.
- Wenn ein Benutzer sein Kennwort vergisst, kann er mit einem Kennwortrücksetzdatenträger wieder Zugang zum Computer erhalten. Ein Administrator kann das Kennwort eines Kontos zwar zurücksetzen, aber dabei können Anmeldeinformationen und verschlüsselte Dateien verloren gehen.
- EFS-Zertifikate lassen sich mit *Certmgr.msc*, *Cipher.exe* oder dem Tool *Dateiverschlüsselungszertifikate verwalten* sichern.
- Mit den Smartcard-Richtlinien können Sie auf einem Windows 7-Computer eine mehrstufige Authentifizierung einführen.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Mehrstufige Authentifizierung**
- **Anhebung der Rechte**
- **Sicherer Desktop**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie Ihr Wissen zum Stoff dieses Kapitels an. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: Benutzerkontensteuerung bei Coho Vineyard

Sie entwickeln für die Windows 7-Computer von Coho Vineyard Richtlinien für die Benutzerkontensteuerung. Die Administratoren müssen Standardbenutzern häufig per Remoteunterstützung helfen. Manchmal ist es erforderlich, dass Administratoren Arbeiten durchführen, die eine Erhöhung der Rechte erfordern. Wenn eine Eingabeaufforderung der Benutzerkontensteuerung erscheint, sollen die Administratoren ihre Anmeldeinformationen eingeben. Allerdings sollen Administratoren andere Teile des Betriebssystems verwenden können, ohne sofort auf die Eingabeaufforderung der Benutzerkontensteuerung zu reagieren. Alle bei Coho Vineyard genehmigten Anwendungen wurden von den Herausgebern der Anwendungen digital signiert.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Welche Richtlinien müssen Sie konfigurieren, um die Anforderungen an die Eingabeaufforderung der Benutzerkontensteuerung für Administratoren zu erfüllen?
2. Welche Richtlinien müssen Sie konfigurieren, damit in einer Remoteunterstützungssitzung eine Anhebung der Rechte möglich ist?
3. Mit welchen Richtlinien stellen Sie sicher, dass nur genehmigte Anwendungen eine Erhöhung der Rechte anfordern können?

Übung 2: Beheben von Kennwortproblemen bei Wingtip Toys

Bei Wingtip Toys haben 20 Leute eigenständige Windows 7-Computer. Einer der Benutzer hat kürzlich sein Kennwort vergessen. Sie konnten das Kennwort des Benutzerkontos zwar zurücksetzen, aber der Benutzer hat den Zugriff auf einige wichtige verschlüsselte Dokumente und seine gespeicherten Website-Anmeldeinformationen verloren. Sie wollen verhindern, dass sich solche Datenverluste wiederholen. Außerdem möchten Sie sicherstellen, dass die Benutzer nicht monatelang dasselbe Kennwort verwenden, wie einige Benutzer es anscheinend getan haben. Die Richtlinien der Firma schreiben einen monatlichen Wechsel des Kennworts vor.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Wie stellen Sie sicher, dass Benutzer nicht den Zugang zu ihren verschlüsselten Dokumenten oder den gespeicherten Anmeldeinformationen verlieren, wenn das Kennwort zurückgesetzt wird?

2. Wie stellen Sie sicher, dass Benutzer auch dann wieder mit möglichst geringem Aufwand Zugang zum Computer erhalten, wenn sie ihre Kennwörter vergessen haben?
3. Wie erreichen Sie, dass Benutzer regelmäßig ihre Kennwörter ändern müssen und nicht immer wieder dieselbe kleine Auswahl von Kennwörtern verwenden?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Konfigurieren der Benutzerkontensteuerung

Führen Sie die erste Übung mit einem der Standardbenutzerkonten durch, die Sie in den bisherigen Übungen angelegt haben. Für die zweite Übung sind zwei Computer erforderlich.

- **Übung 1** Stellen Sie in der Konsole *Lokale Sicherheitsrichtlinie* die Richtlinien für die Benutzerkontensteuerung so ein, dass Standardbenutzer zur Eingabe von Anmeldeinformationen aufgefordert werden, wenn sie eine Arbeit durchführen wollen, für die erhöhte Rechte erforderlich sind, wie zum Beispiel die Öffnung einer Eingabeaufforderung mit erhöhten Rechten.
- **Übung 2** Stellen Sie in der Konsole *Lokale Sicherheitsrichtlinie* die Richtlinien für die Benutzerkontensteuerung so ein, dass ein Helfer in der Eingabeaufforderung der Benutzerkontensteuerung seine Anmeldeinformationen eingeben kann, wenn er in einer Remoteunterstützungssitzung remote verbunden ist. Versenden Sie die Einladung zur Remoteunterstützung auf dem Computer *Aberdeen*, den Sie in Kapitel 6, »Netzwerkeinstellungen«, eingerichtet haben.

Konfigurieren der Authentifizierung und Autorisierung

Sie sollten beide Übungen durchführen. Für die erste Übung ist ein Diskettenlaufwerk oder ein USB-Speichergerät erforderlich.

- **Übung 1** Erstellen Sie für ein anderes Benutzerkonto als *Kim_Akers* eine Kennwortrücksetzdiskette. Verwenden Sie die Kennwortrücksetzdiskette, um sich mit dem betreffenden Konto anzumelden.
- **Übung 2** Sichern Sie ein EFS-Zertifikat mit dem Tool *Dateiverschlüsselungszertifikate verwalten*.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

KAPITEL 10

DirectAccess und VPN-Verbindungen

Virtuelle private Netzwerke (VPNs) ermöglichen den Remotezugriff auf den Arbeitsplatz, unabhängig davon, ob man gerade im Café um die Ecke sitzt oder am anderen Ende der Welt auf den nächsten Flug wartet. Wenn die Infrastruktur im Büro richtig aufgebaut ist, brauchen Sie nur Zugang zum Internet, um ein VPN verwenden zu können.

In diesem Kapitel erfahren Sie etwas über die neuen VPN-Technologien von Windows 7 und über andere Technologien, die Ihnen vielleicht schon geläufig sind. Eine davon ermöglicht es dem Windows 7-Computer, eine Verbindung automatisch wiederherzustellen, falls sie unterbrochen wird oder Sie von einem Internetanbieter zum nächsten wechseln. DirectAccess ist eine andere VPN-Lösung, die eine ständige Verbindung zum Firmennetzwerk ermöglicht, sobald der Windows 7-Client eine Verbindung mit dem Internet erkennt. Wenn Sie dieses Kapitel durcharbeiten, erfahren Sie auch, wie Sie mit Clients umgehen, die gewartet werden müssen, bevor sie auf ein Netzwerk mit Netzwerkzugriffsschutz zugreifen können, und wie Sie Remotedesktopverbindungen mit internen Netzwerkservern konfigurieren, ohne VPN-Verbindungen einrichten zu müssen.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von DirectAccess
- Konfigurieren von Remoteverbindungen

Lektionen in diesem Kapitel:

- Lektion 1: Verwalten von DirectAccess 515
- Lektion 2: Remoteverbindungen 530

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels sind einige Vorbereitungen erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Client-PC namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.
- Um die Übungen in Lektion 2 durchführen zu können, sollten Sie dafür sorgen, dass der Windows 7-Computer *Canberra* über eine aktive Internetverbindung verfügt.

Praxistipp

Orin Thomas

Der größte Nachteil der Tatsache, überall arbeiten zu können, besteht darin, überall arbeiten zu können. Ich habe mich schon an vielen seltsamen Orten bei der Arbeit ertappt, angefangen bei der Wartehalle in Bangkok, wo ich auf einen Flug nach Kopenhagen wartete, bis hin zum Balkon eines Hotels, das sich auf einer Insel mitten im Great Barrier Reef befand. Ich rede mir immer ein, ich würde nur ein paar Augenblicke arbeiten, um mit der Arbeit nicht zu sehr in Verzug zu kommen. Die Hamster in Laufrädern haben wahrscheinlich ähnliche Ausreden. Während es in der Vergangenheit recht leicht war, einfach abzuschalten, verfügen Sie heute im Bereich eines Sendemastes gewöhnlich über Internetzugriff und über VPN-Verbindungen, mit denen Sie eine Verbindung zum Büro herstellen können. Anders gesagt, das Büro ist, wo Sie sind. Die Arbeit endet nicht mehr mit dem verlassen des Büros. Das Büro ist überall, wo es das Internet gibt. Durch einige der in diesem Kapitel beschriebenen Technologien verschwimmen die Grenzen zwischen Privatleben und Arbeit noch weiter. Wenn wir über diese Technologien reden, geht es uns hauptsächlich um die Möglichkeit, auf Geschäftsreisen eine Verbindung mit dem Firmennetzwerk herzustellen. In der Praxis stellt man allerdings fest, dass viele Leute die Remotezugriffstechnologie dazu verwenden, um nach Feierabend eine Verbindung mit dem Büro herzustellen und noch etwas mehr Arbeit zu erledigen. Im letzten Jahrzehnt wurde es immer schwieriger, zwischen Arbeit und Freizeit einen klaren Trennungsstrich zu ziehen. Die in diesem Kapitel besprochenen Technologien verstärken diese Tendenz.

Lektion 1: Verwalten von DirectAccess

DirectAccess ist eine neue Technologie in Windows 7, die irgendwann vielleicht herkömmliche VPN-Lösungen wie PPTP (Point-to-Point Tunneling Protocol), L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security) und SSTP (Secure Socket Tunneling Protocol) ersetzt. DirectAccess ist eine Lösung für automatische Verbindungen, die es Windows 7-Clients ermöglicht, von dem Moment an, in dem eine Verbindung mit dem globalen Internet zustande kommt, nahtlos eine Verbindung mit dem Intranet des Unternehmens herzustellen. Die Umstellung von herkömmlichen Lösungen auf DirectAccess wird nicht über Nacht erfolgen. Organisationen müssen beträchtliche Änderungen in ihrer Netzwerkinfrastruktur durchführen, neue Client- und Servertechnologien einsetzen und IPv6 verwenden. In dieser Lektion erfahren Sie etwas über die Vorteile und die technologischen Voraussetzungen von DirectAccess, und was Sie in Ihrer Organisation tun müssen, um es zu implementieren.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren von DirectAccess-Clients mit Netsh
- Konfigurieren der DirectAccess-Authentifizierung
- Beschreiben der Infrastrukturvoraussetzungen für DirectAccess

Veranschlagte Zeit für diese Lektion: 30 Minuten

Grundlagen von DirectAccess

DirectAccess ist eine IPv6-VPN-Verbindung, die mit IPsec geschützt wird und verfügbar ist, sobald eine Internetverbindung besteht. Wenn ein entsprechend konfigurierter Computer eine Verbindung mit dem Internet herstellen kann, verbindet DirectAccess diesen Computer automatisch mit einem entsprechend konfigurierten Firmennetzwerk. DirectAccess unterscheidet sich in folgenden Punkten von den VPN-Lösungen, die in Lektion 2, »Remoteverbindungen«, besprochen werden:

- Die Verbindung wird automatisch hergestellt und erfordert kein Eingreifen des Benutzers und keine Anmeldung. Der Aufbau der DirectAccess-Verbindung beginnt in dem Moment, in dem der Computer eine Verbindung mit einem aktiven Netzwerk hergestellt hat. Aus der Sicht des Benutzers verfügt der Computer immer über Zugang zum Firmennetzwerk, ob der Benutzer nun im Büro sitzt oder in einem Strandcafé eine Verbindung mit einem Wi-Fi-Hotspot hergestellt hat. Bisher mussten VPN-Verbindungen mit dem Intranet der Firma manuell hergestellt werden.
- DirectAccess ist bidirektional, wobei die Server aus dem Intranet in der gleichen Weise mit dem Windows 7-Client kommunizieren können, wie es bei einem direkten Anschluss des Clients am LAN (Local Area Network) möglich wäre. Bei vielen herkömmlichen VPN-Lösungen haben Clients zwar Zugang zum Intranet, aber Server aus dem Intranet können keine Verbindung zum Client aufbauen.
- DirectAccess bietet Administratoren größere Kontrolle darüber, welche Ressourcen aus dem Intranet für Remotebenutzer und -computer verfügbar sind. Sie können DirectAccess mit dem Netzwerkzugriffsschutz (Network Access Protection, NAP) kombinieren, um sicherzustellen, dass Remoteclients auf dem neusten Stand bleiben, was Virendefinitionen und Softwareupdates betrifft. Außerdem können Administratoren Verbindungssicherheitsrichtlinien anwenden, um Server und Hosts zu isolieren.



Weitere Informationen Überblick über DirectAccess für Führungskräfte

Weitere Informationen über die Grundlagen von DirectAccess finden Sie im Dokument *DirectAccess Executive Overview*, das Sie von der Microsoft-Website herunterladen können: *http://www.microsoft.com/downloads/details.aspx?FamilyID=D8EB248B-8BF7-4798-A1D1-04D37F2E013C&displaylang=en.*

Der DirectAccess-Verbindungsaufbau

Der DirectAccess-Verbindungsaufbau erfolgt automatisch, erfordert also kein Eingreifen der Person, die sich am Windows 7-Computer anmeldet. Ein portabler Computer, der in die Privatwohnung mitgenommen wird und dort Internetzugang erhält, kann selbst dann Software- und Gruppenrichtlinienupdates von den Servern aus dem Firmennetzwerk erhalten, wenn sich kein Benutzer angemeldet hat. Windows 7-Clients stellen auf folgende Weise eine DirectAccess-Verbindung her:

1. Der mit DirectAccess konfigurierte Windows 7-Client stellt eine Verbindung mit einem Netzwerk her. In den meisten Fällen geschieht dies, bevor sich ein Benutzer am Computer anmeldet.
2. Wenn der Client während der Netzwerkidentifikationsphase erkennt, dass er mit einem neuen Netzwerk verbunden ist oder eine bereits hergestellte Verbindung mit einem vorhandenen Netzwerk wieder aufnimmt, versucht er, eine Verbindung mit einer speziell konfigurierten Intranetwebsite herzustellen. Ein Administrator legt diese Websiteadresse fest, wenn er auf dem DirectAccess-Server DirectAccess konfiguriert. Wie das geschieht, erfahren Sie im Verlauf dieser Lektion. Kann der Client Kontakt zu dieser Website herstellen, schließt Windows 7 daraus, dass bereits eine Verbindung mit dem Firmennetzwerk besteht und keine weitere Aktion erforderlich ist.
3. Wenn der Client keinen Kontakt zu der speziell konfigurierten Intranetwebsite herstellen kann, überprüft er, ob ein IPv6-Netzwerk vorliegt. Liegt ein IPv6-Netzwerk vor und wurde dem Client eine öffentliche IPv6-Adresse zugewiesen, stellt DirectAccess über das Internet eine direkte Verbindung zum DirectAccess-Server her.
4. Ist kein IPv6-Netzwerk vorhanden, versucht Windows 7, einen IPv6-über-IPv4-Tunnel einzurichten, zuerst mit IP6-zu-IP4 und dann mit Teredo. Die Übergangstechnologien Teredo und IP6-zu-IP4 haben Sie bereits in Kapitel 6, »Netzwerkeinstellungen«, kennen gelernt.
5. Wenn der Windows 7-Client wegen einer Firewall oder eines Proxyservers keine Teredo- oder IP6-zu-IP4-Verbindung herstellen kann, versucht er, eine Verbindung mit IP-HTTPS herzustellen. IP-HTTPS (Internet Protocol-Hypertext Protocol Secure) kapselt IPv6-Datenverkehr über eine HTTPS-Verbindung. Die Wahrscheinlichkeit für eine erfolgreiche Verbindung mit IP-HTTPS ist ziemlich hoch, weil nur wenige Firewalls, die Verbindungen ins Internet zulassen, den Datenverkehr auf TCP-Port 443 blockieren.
6. Die DirectAccess-IPsec-Sitzung wird eingerichtet, wenn sich der Windows 7-Client und der DirectAccess-Server gegenseitig mit ihren Computerzertifikaten authentifiziert haben. DirectAccess unterstützt nur eine Authentifizierung mit Zertifikaten.
7. Der DirectAccess-Server überprüft in der entsprechenden Active Directory-Domänendienstegruppe (Active Directory Domain Services, AD DS), ob der Computer und der Benutzer für eine Verbindung mit DirectAccess autorisiert sind.

8. Nun verfügt der DirectAccess-Client über Zugang zu den entsprechend konfigurierten Ressourcen aus dem Firmennetzwerk.

Tabelle 10.1 fasst die DirectAccess-Clientkonfigurationen und die entsprechenden Methoden zur Kommunikation mit dem DirectAccess-Server zusammen. Wenn Sie den DirectAccess-Server konfigurieren, dann konfigurieren Sie ihn für alle diese verschiedenen Verbindungsmethoden. Das ist sinnvoll, weil Sie nicht vorhersehen können, welche Verhältnisse in den Remotenetzwerken gelten, von denen aus DirectAccess-Clients Verbindungen herstellen. IP-HTTPS wird zuletzt probiert, weil die anderen Methoden eine bessere Leistung aufweisen.

Tabelle 10.1 DirectAccess-Verbindungsmethoden

Client-Netzwerkverbindung	DirectAccess-Verbindungsmethode
Öffentliche IPv6-Adresse	Öffentliche IPv6-Adresse
Öffentliche IPv4-Adresse	IP6-zu-IP4
Private IPv4-Adresse (NAT)	Teredo
Der Client ist mit dem Internet verbunden, kann aber wegen der Firewall keine DirectAccess-Verbindung herstellen	IP-HTTPS

Konfigurieren des DirectAccess-Clients

Nur Clientcomputer, die Mitglieder einer Domäne sind und auf denen die Editionen Windows 7 Enterprise oder Ultimate ausgeführt werden, unterstützen DirectAccess. Auf anderen Editionen von Windows 7 oder auf älteren Windows-Versionen wie etwa Windows Vista oder Windows XP können Sie DirectAccess nicht verwenden. Wenn Sie einen Client für DirectAccess konfigurieren, müssen Sie das Domänencomputerkonto des Clients zu einer speziellen Sicherheitsgruppe hinzufügen. Diese Sicherheitsgruppe geben Sie an, wenn Sie den DirectAccess-Server mit dem DirectAccess-Assistenten konfigurieren. Die Konfiguration dieser speziellen Gruppe wird im Verlauf der Lektion noch beschrieben.

Clients erhalten ihre DirectAccess-Konfiguration über Gruppenrichtlinien. Herkömmliche VPN-Verbindungen werden dagegen manuell konfiguriert oder mit dem Verbindungs-Manager-Verwaltungskit verteilt. Nachdem Sie das Computerkonto des Clients zur vorgesehenen Sicherheitsgruppe hinzugefügt haben, müssen Sie auf dem Client ein Computerzertifikat für die DirectAccess-Authentifizierung installieren. In der Infrastruktur der Organisation müssen die Active Directory-Zertifikatdienste bereitgestellt werden, damit Clients die erforderlichen Zertifikate automatisch anfordern können.

Manuelles Konfigurieren von DirectAccess

Wie bereits erwähnt, erhalten DirectAccess-Clients ihre Konfiguration über Gruppenrichtlinien. Diese Gruppenrichtlinien werden so gefiltert, dass sie nur für Computer gelten, die Mitglieder bestimmter DirectAccess-Sicherheitsgruppen sind. Sie finden diese Richtlinien im Knoten *Computerkonfiguration\(Richtlinien\)Administrative Vorlagen\Netzwerk\TCP/IP-Einstellungen\IPv6-Übergangstechnologien* (Abbildung 10.1).

Da Computer Mitglieder von Domänen sein und zu bestimmten Sicherheitsgruppen hinzugefügt werden müssen, die speziell für DirectAccess eingerichtet wurden, hat es wenig Sinn, wenn ein lokaler Administrator auf einzelnen Windows 7-Clients die DirectAccess-Einstellungen in den lokalen Gruppenrichtlinien ändert.

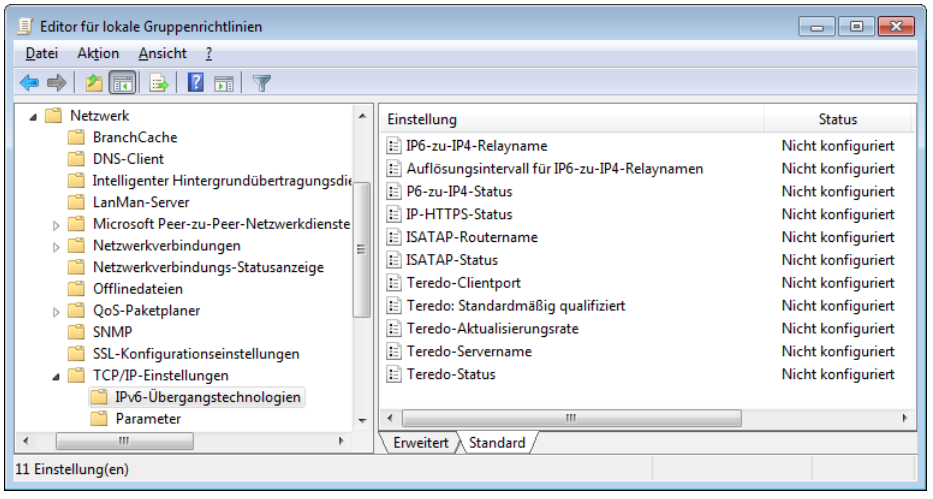


Abbildung 10.1 DirectAccess-Gruppenrichtlinien

Wenn Sie auf dem DirectAccess-Server DirectAccess einrichten, wird auf Domänenebene ein Gruppenrichtlinienobjekt erstellt, das für eine bestimmte Sicherheitsgruppe gilt. Dieses GPO wendet folgende Richtlinien an:

- **IP6-zu-IP4-Relayname** Diese Richtlinie legt den IP6-zu-IP4-Relaynamen fest und wird so konfiguriert, dass eine der öffentlichen IPv4-Adressen für den DirectAccess-Server verwendet wird.
- **IP-HTTPS-Status** Diese Richtlinie legt die URL (Uniform Resource Locator) des IP-HTTPS-Servers fest. Dabei handelt es sich um den FQDN einer der öffentlichen IPv4-Adressen des DirectAccess-Servers. Die Standardeinstellung sieht IP-HTTPS als letzte Wahl vor. Es ist möglich, diese Richtlinie so einzustellen, dass IP-HTTPS immer verwendet wird, selbst wenn andere Verbindungsoptionen wie IP6-zu-IP4 oder Teredo verfügbar sind.
- **Teredo: Standardmäßig qualifiziert** Diese Richtlinie legt fest, ob Teredo verwendet wird. Für DirectAccess-Clients wird die Richtlinie aktiviert.
- **Teredo-Servername** Diese Richtlinie legt den Namen des Teredo-Servers fest. Diesem Namen wird eine der öffentlichen IPv4-Adressen des DirectAccess-Server zugeordnet.

Die letzte Richtlinie, die bei der Einrichtung des DirectAccess-Servers konfiguriert wird, ist die *Namensauflösungsrichtlinie*. Sie ist unter *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Namensauflösungsrichtlinie* zu finden (Abbildung 10.2).

Es ist zwar möglich, DirectAccess-Einstellungen mit dem Befehlszeilenprogramm Netsh vorzunehmen, aber Gruppenrichtlinieneinstellungen haben Vorrang vor Einstellungen, die manuell mit Netsh durchgeführt werden. Die Befehle zur Konfiguration der DirectAccess-Einstellungen lauten wie folgt:

```
Netsh interface ipv6 set teredo enterpriseclient IPv4_Adresse
Netsh interface 6to4 set relay IPv4_Adresse
Netsh interface httpstunnel add interface client https://fqdn/IPHTTPS
```

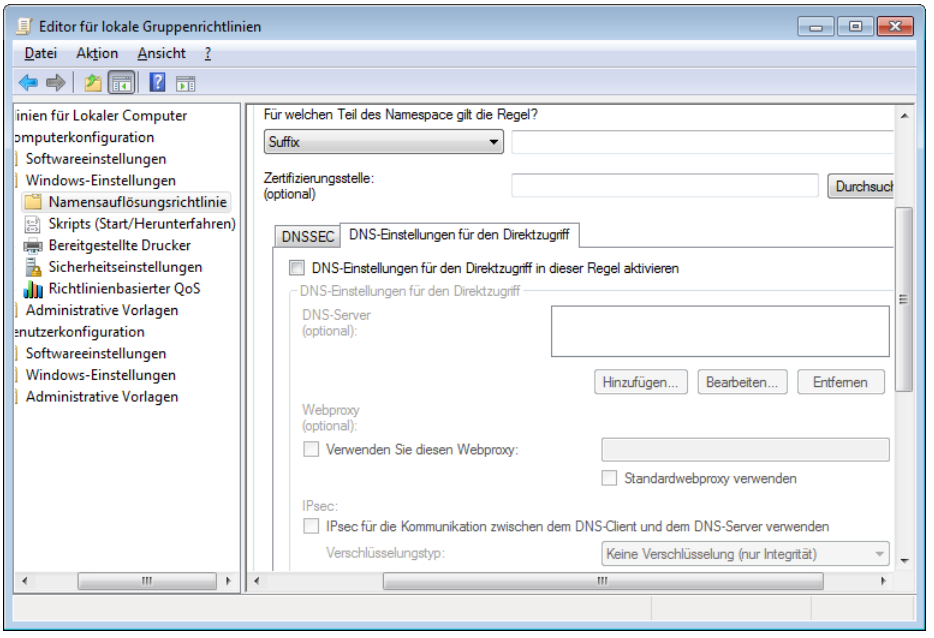


Abbildung 10.2 DirectAccess-Namensauflösung

Der erste Befehl konfiguriert Teredo. Bei der IPv4-Adresse, die Sie mit diesem Befehl zuweisen, handelt es sich um eine der öffentlichen IPv4-Adressen des DirectAccess-Servers. Der zweite Befehl konfiguriert IP6-zu-IP4 und verwendet ebenfalls eine der öffentlichen IPv4-Adressen des DirectAccess-Servers. Der letzte Befehl konfiguriert IP-HTTPS. Sie sollten den FQDN verwenden, der mit einer der öffentlichen IPv4-Adressen verknüpft ist und für den auf dem DirectAccess-Server ein SSL-Zertifikat vorliegt.



Weitere Informationen **Manuelles Konfigurieren von DirectAccess-Clients**

Weitere Informationen über das manuelle Konfigurieren von DirectAccess-Clients erhalten Sie in folgendem Microsoft TechNet-Dokument: *http://technet.microsoft.com/de-de/library/dd637798.aspx*.

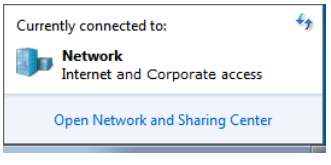


Abbildung 10.3 Die Meldung »Internet and Corporate Access«

Beheben von DirectAccess-Problemen

Ob ein Client erfolgreich eine DirectAccess-Verbindung hergestellt hat, können Sie mit einem Klick auf das Symbol *Netzwerk*-Symbol überprüfen. Lautet die Statusmeldung »Internet and Corporate Access« (Abbildung 10.3), konnte der Windows 7-Computer eine

DirectAccess-Verbindung herstellen. Lautet die Statusmeldung »Local and Internet Access«, besteht keine Verbindung zum DirectAccess-Server.

Wie bereits erwähnt, verwenden DirectAccess-Clients für die Authentifizierung mit dem DirectAccess-Server digitale Zertifikate. Wenn ein Computer nicht über ein gültiges Computerzertifikat verfügt, das von einer Zertifizierungsstelle ausgestellt wurde, der der DirectAccess-Server zu Authentifizierungszwecken vertraut, kann keine Verbindung hergestellt werden. DirectAccess-Clients und der DirectAccess-Server erhalten ihre Zertifikate gewöhnlich von einer Zertifizierungsstelle, die mit den Active Directory-Zertifikatdiensten aufgebaut wurde und zur Domäne gehört. Damit ist sichergestellt, dass Client und Server den Zertifikaten des anderen vertrauen. So können Sie überprüfen, ob auf einem Windows 7-Client ein entsprechendes Computerzertifikat vorhanden ist:

1. Öffnen Sie die Microsoft Management Console, indem Sie im Textfeld *Programme/Dateien durchsuchen* **mmc** eingeben.
2. Fügen Sie das Snap-In *Zertifikate* für das lokale Computerkonto hinzu.
3. Navigieren Sie zum Knoten *Zertifikate (Lokaler Computer)\Eigene Zertifikate\Zertifikate* und überprüfen Sie, ob auf dem Computer ein Zertifikat für die Verwendungszwecke Clientauthentifizierung und Serverauthentifizierung vorhanden ist (Abbildung 10.4).

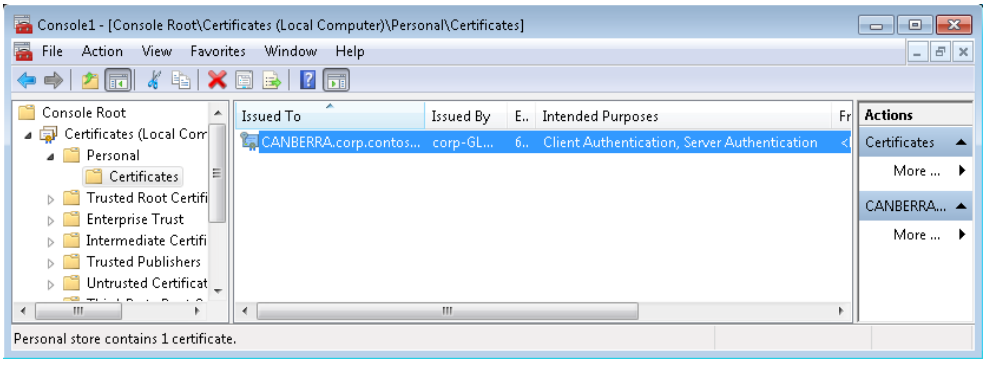


Abbildung 10.4 Überprüfen des DirectAccess-Clientzertifikats

Die DirectAccess-Konfiguration können Sie mit mehreren Befehlszeilenprogrammen überprüfen. Zur Überprüfung der Einstellungen des DirectAccess-Clients für IP6-zu-IP4 verwenden Sie folgenden Befehl:

```
Netsh interface 6to4 show relay
```

Wenn ein Client seine DirectAccess-Konfiguration über Gruppenrichtlinien erhalten hat, zeigt dieser Befehl eine der öffentlichen IPv4-Adressen an, die dem DirectAccess-Server als Relayadresse zugewiesen wurde. Wenn die Relayeinstellung *Default* lautet, wurden die DirectAccess-Gruppenrichtlinien nicht korrekt angewendet. In ähnlicher Weise sollten Sie eine der beiden öffentlichen Adressen des DirectAccess-Servers bei der Überprüfung der Teredo-Konfiguration sehen, wenn die DirectAccess-Konfiguration über Gruppenrichtlinien angewendet wird. Die Teredo-Konfiguration können Sie mit folgendem Befehl überprüfen:

```
Netsh interface ipv6 show teredo
```

Über die IP-HTTPS-Konfiguration erhalten Sie mit folgendem Befehl Informationen:

```
Netsh interface httpstunnel show interfaces
```



Weitere Informationen Beheben von DirectAccess-Problemen

Weitere Informationen über das Beheben von DirectAccess-Problemen erhalten Sie in folgendem Microsoft TechNet-Dokument: *http://technet.microsoft.com/en-us/library/dd637786.aspx*.

Schnelltest

- Welche IPv6-Übergangstechnologie verwendet DirectAccess, wenn Sie sich an einem Remotestandort befinden und Ihrem Computer eine öffentliche IPv4-Adresse, aber keine öffentliche IPv6-Adresse zugewiesen wurde?

Antwort zum Schnelltest

- DirectAccess verwendet die IP6-zu-IP4-Übergangstechnologie, wenn dem Client eine öffentliche IPv4-Adresse, aber keine öffentliche IPv6-Adresse zugewiesen wurde.

Konfigurieren des DirectAccess-Servers

Die Konfiguration von DirectAccess erfolgt hauptsächlich auf dem DirectAccess-Server. Bei der Einrichtung des Servers konfigurieren Sie die erforderlichen Gruppenrichtlinienobjekte, die DirectAccess unterstützen. Vor der Installation von DirectAccess sollten Sie dafür sorgen, dass der DirectAccess-Server folgende Voraussetzungen erfüllt:

- Auf dem Computer muss Windows Server 2008 R2 installiert sein und er muss Mitglied einer Domäne sein.
- Der Server muss über zwei Netzwerkkarten verfügen.
- Über eine dieser Netzwerkkarten muss eine direkte Verbindung mit dem Internet hergestellt werden können. Dieser Netzwerkkarte müssen Sie zwei aufeinanderfolgende öffentliche IPv4-Adressen zuweisen.
- Die zweite Netzwerkkarte braucht eine direkte Verbindung zum Intranet der Organisation.
- Der Computer braucht ein digitales Zertifikat zur Serverauthentifizierung. Dazu ist ein Computerzertifikat erforderlich, das auf den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) ausgestellt ist, der den IP-Adressen der externen Netzwerkschnittstelle des DirectAccess-Servers zugewiesen wurde.

Sie müssen in AD DS außerdem mindestens eine globale Sicherheitsgruppe für DirectAccess erstellen. Die Gruppe kann zwar einen beliebigen Namen tragen, aber die Verhältnisse werden übersichtlicher, wenn schon ihr Name auf die Verwendung für DirectAccess hinweist. Bei Bedarf können Sie mehrere Sicherheitsgruppen für DirectAccess erstellen. Das könnte beispielsweise erforderlich sein, um Zugriff auf verschiedene Segmente des Intranets zu konfigurieren.

Zur Installation von DirectAccess auf einem Server, auf dem Windows Server 2008 R2 ausgeführt wird, fügen Sie im Assistenten zum Hinzufügen von Features das Feature *DirectAccess-Verwaltungskonsole* hinzu (Abbildung 10.5). Die DirectAccess-Verwaltungskonsole ermöglicht die Konfiguration und Verwaltung der DirectAccess-Funktionen. Außerdem müssen Sie das Feature *Gruppenrichtlinienverwaltung* hinzufügen, weil der DirectAccess-Installationsassistent Gruppenrichtlinienobjekte für DirectAccess erstellt, mit denen DirectAccess-Clients konfiguriert werden. Sie müssen den DirectAccess-Installationsassistenten mit einem Benutzerkonto ausführen, das über die Berechtigung verfügt, in der Domäne Gruppenrichtlinienobjekte zu erstellen und anzuwenden.

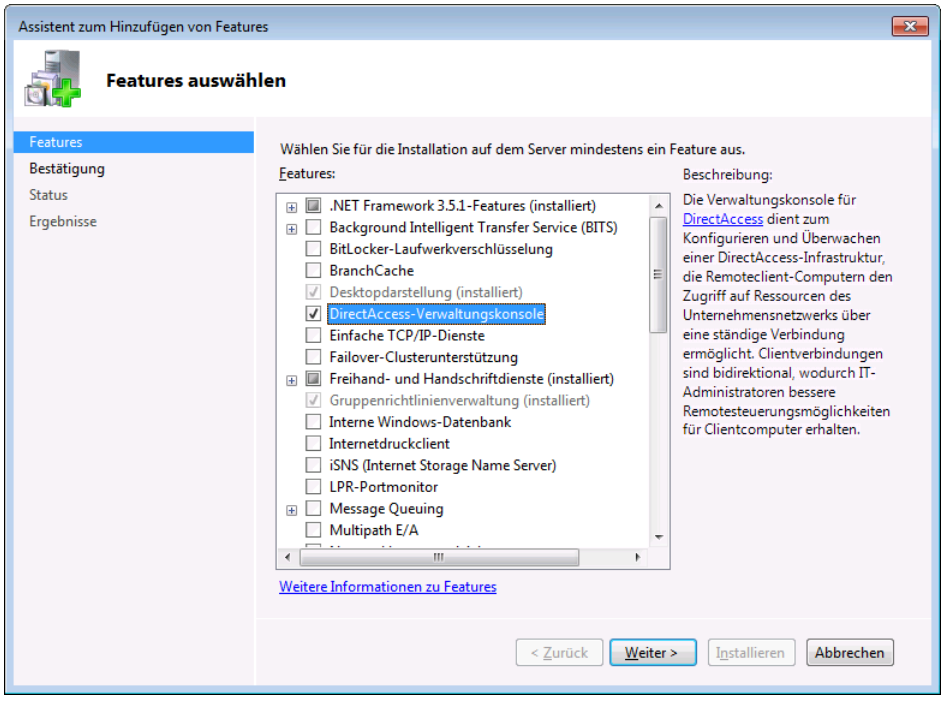


Abbildung 10.5 Installieren des Features *DirectAccess* unter Windows Server 2008 R2

Nach der Installation der DirectAccess-Verwaltungskonsole können Sie den DirectAccess-Server konfigurieren:

1. Öffnen Sie die DirectAccess-Verwaltungskonsole im Menü *Verwaltung* (Abbildung 10.6).
2. Wählen Sie den Knoten *Setup*. Klicken Sie im Detailbereich unter *Remote Clients* auf *Configure*. Es öffnet sich das Dialogfeld *DirectAccess-Clientsetup*. Klicken Sie auf *Hinzufügen* und geben Sie dann den Namen der Sicherheitsgruppe an, zu der die Computerkonten der Windows 7-Clients, die DirectAccess-Zugriff erhalten sollen, hinzugefügt werden sollen. Die Gruppen können beliebige Namen erhalten. In Abbildung 10.7 heißt die Gruppe *DA_Clients*.

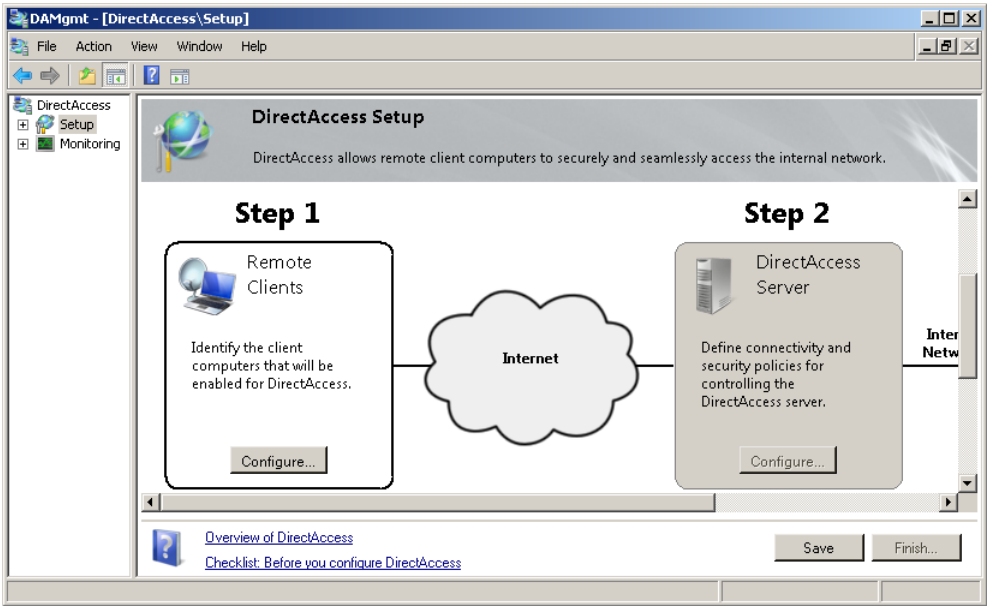


Abbildung 10.6 DirectAccess-Verwaltungskonsole

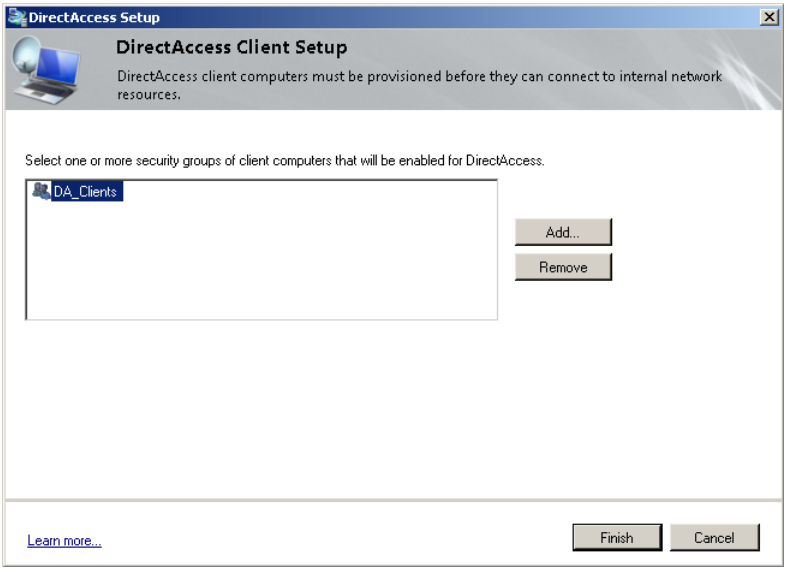

DirectAccess Setup
DirectAccess Client Setup
DirectAccess client computers must be provisioned before they can connect to internal network resources.
Select one or more security groups of client computers that will be enabled for DirectAccess.
DA_Clients
Add...
Remove
Learn more...
Finish
Cancel

Abbildung 10.7 DirectAccess-Clientgruppen

3. Verwenden Sie das Element *DirectAccess-Serversetup*, um anzugeben, welche Schnittstelle mit dem Internet verbunden ist und welche Schnittstelle mit dem internen Netzwerk verbunden ist. Durch diesen Schritt werden die IPv6-Übergangstechnologien auf dem DirectAccess-Server aktiviert (Abbildung 10.8). Im nächsten Schritt geben Sie an, von welcher Zertifizierungsstelle die Clientzertifikate stammen müssen, sei es direkt

oder durch eine untergeordnete Zertifizierungsstelle ausgestellt. Außerdem müssen Sie das Serverzertifikat angeben, mit dem IP-HTTPS-Datenverkehr gesichert werden soll.

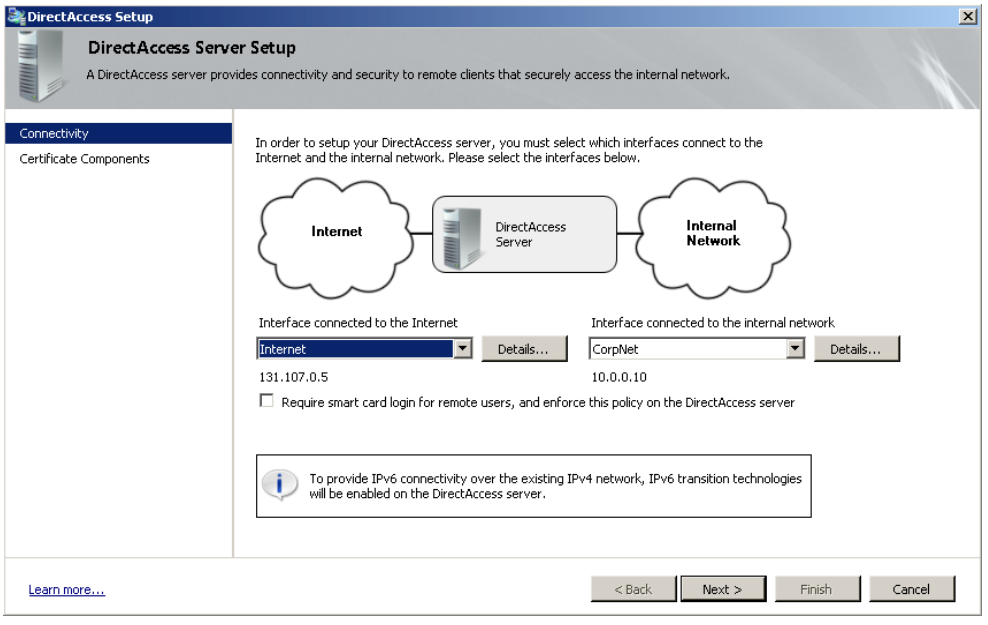

DirectAccess Setup
DirectAccess Server Setup
A DirectAccess server provides connectivity and security to remote clients that securely access the internal network.
Connectivity
Certificate Components
In order to setup your DirectAccess server, you must select which interfaces connect to the Internet and the internal network. Please select the interfaces below.
Internet
DirectAccess Server
Internal Network
Interface connected to the Internet
Internet
Details...
131.107.0.5
Interface connected to the internal network
CorpNet
Details...
10.0.0.10
Require smart card login for remote users, and enforce this policy on the DirectAccess server
To provide IPv6 connectivity over the existing IPv4 network, IPv6 transition technologies will be enabled on the DirectAccess server.
Learn more...
< Back
Next >
Finish
Cancel

Abbildung 10.8 *DirectAccess-Serversetup*

4. Auf der Seite *Infrastrukturserver-Setup* geben Sie eine interne Website an (den Netzwerkadressenserver). DirectAccess-Clients versuchen, mit dieser Website Kontakt aufzunehmen und herauszufinden, ob sie direkt mit dem Intranet der Organisation verbunden sind oder sich an einem Remotestandort befinden. Sie müssen diese Website mit einem *Webserver*-Zertifikat sichern (Abbildung 10.9). In diesem Dialogfeld geben Sie auch an, welche DNS-Server und Domänencontroller zu Authentifizierungszwecken für die DirectAccess-Clients zur Verfügung stehen.
5. Im letzten Schritt geben Sie an, welche Ressourcen aus dem Intranet der Organisation für DirectAccess-Clients verfügbar sind. Die Standardeinstellung lässt Zugriffe auf alle Ressourcen zu. In einer Umgebung mit höheren Sicherheitsanforderungen ist es möglich, den Kontakt mit Isolationsrichtlinien auf Mitglieder bestimmter Sicherheitsgruppen einzuschränken. Sie können zum Beispiel eine Sicherheitsgruppe erstellen und dann die Computerkonten von ausgewählten Datei- und E-Mail-Servern hinzufügen.
6. Wenn Sie auf *Fertig stellen* klicken, stellt DirectAccess Kontakt zu einem Domänencontroller her und erstellt in der Domäne zwei neue Gruppenrichtlinienobjekte. Das erste ist für Sicherheitsgruppen vorgesehen, zu denen die Computerkonten der DirectAccess-Clients gehören. Das zweite Gruppenrichtlinienobjekt ist für den DirectAccess-Server vorgesehen. Abbildung 10.10 zeigt diese Gruppenrichtlinienobjekte.

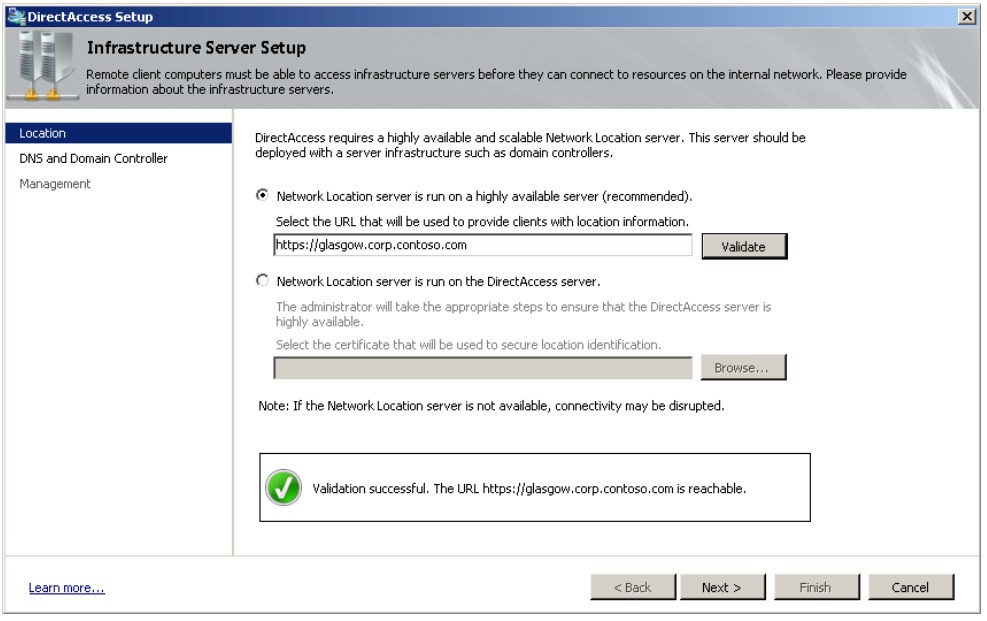

DirectAccess Setup
Infrastructure Server Setup
Remote client computers must be able to access infrastructure servers before they can connect to resources on the internal network. Please provide information about the infrastructure servers.
Location
DNS and Domain Controller
Management
DirectAccess requires a highly available and scalable Network Location server. This server should be deployed with a server infrastructure such as domain controllers.
Network Location server is run on a highly available server (recommended).
Select the URL that will be used to provide clients with location information.
https://glasgow.corp.contoso.com
Validate
Network Location server is run on the DirectAccess server.
The administrator will take the appropriate steps to ensure that the DirectAccess server is highly available.
Select the certificate that will be used to secure location identification.
Browse...
Note: If the Network Location server is not available, connectivity may be disrupted.
Validation successful. The URL https://glasgow.corp.contoso.com is reachable.
Learn more...
< Back
Next >
Finish
Cancel

Abbildung 10.9 Angeben des Netzwerkadressenservers

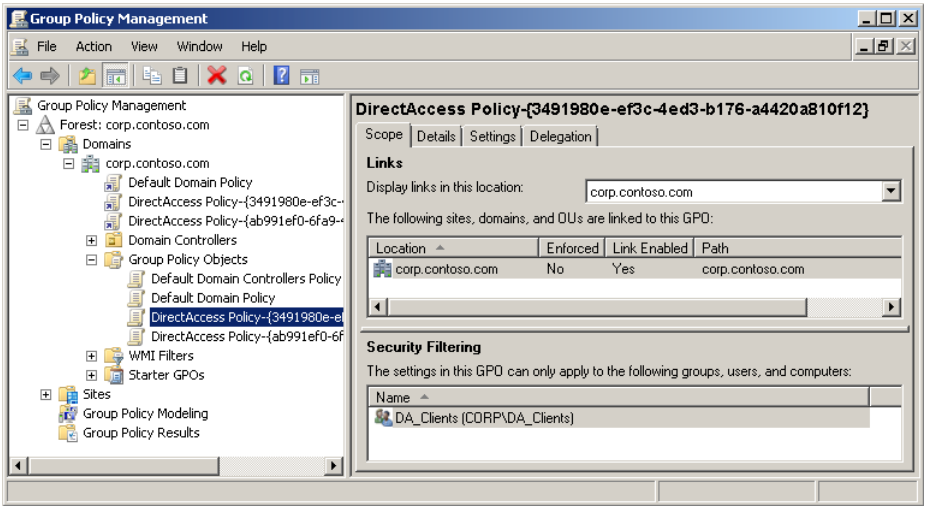


Abbildung 10.10 DirectAccess-GPOs

DirectAccess ist auf einige andere Komponenten der Netzwerkinfrastruktur angewiesen. In der Domäne, in der Sie den DirectAccess-Server installieren, müssen folgende Komponenten zur Verfügung stehen:

- Mindestens ein Domänencontroller, auf dem Windows Server 2008 R2 ausgeführt wird und ein DNS-Server eingerichtet ist.
- Ein Windows Server 2008-Server mit installierten Active Directory-Zertifikatdiensten, entweder als Unternehmens-Stammzertifizierungsstelle oder als eine untergeordnete Unternehmenszertifizierungsstelle.

Damit interne Netzwerkressourcen für DirectAccess-Remoteclients verfügbar werden, müssen Sie eine der folgenden Vorbereitungen treffen:

- Sorgen Sie dafür, dass alle internen Ressourcen, die mit DirectAccess verwendet werden, IPv6 unterstützen.
- Stellen Sie ISATAP im Intranet bereit. ISATAP ermöglicht den Zugang zu Intranetservern und -anwendungen, indem für IPv6-Datenverkehr ein Tunnel durch das IPv4-Intranet eingerichtet wird.
- Stellen Sie ein NAT-PT-Gerät bereit. NAT-PT-Geräte machen es möglich, dass DirectAccess-Clients, die IPv6 verwenden, Hosts erreichen, die nur IPv4-Adressen unterstützen.

Alle Anwendungsserver, die für DirectAccess-Clients zugänglich sein sollen, müssen in der Windows-Firewall mit erweiterter Sicherheit (WFAS) ICMPv6-Datenverkehr zulassen. Dazu können Sie in den Gruppenrichtlinien folgende Firewallregeln zulassen.

- Eingehende ICMPv6-Echoanforderungsmeldungen
- Ausgehende ICMPv6-Echoanforderungsmeldungen

Die folgenden Ports müssen in der externen Firewall der Organisation geöffnet sein, um DirectAccess zu unterstützen:

- **UDP-Port 3544** Ermöglicht Teredo-Datenverkehr
- **IPv4-Protokoll 41** Ermöglicht IP6-zu-IP4-Datenverkehr
- **TCP-Port 443** Ermöglicht IP-HTTPS-Datenverkehr
- **ICMPv6- und IPv4-Protokoll 50** Erforderlich, wenn die Remoteclients über IPv6-Adressen verfügen



Prüfungstipp

Merken Sie sich, unter welchen Bedingungen die Verwendung von Teredo, IP6-zu-IP4 und IP-HTTPS auf DirectAccess-Clients erforderlich wird.

Übung Konfigurieren von DirectAccess mit Netsh

DirectAccess erfordert eine Netzwerkinfrastruktur mit Windows Server 2008 R2. Es ist also nicht möglich, auf einem Windows 7-Client mit DirectAccess zu arbeiten, ohne über einige Server zu verfügen, auf denen Windows Server 2008 R2 ausgeführt wird. In dieser Übung simulieren Sie die manuelle Konfiguration verschiedener IPv6-DirectAccess-Komponenten mit Netsh.

Übung 1 DirectAccess-Konfiguration mit Netsh

In dieser Übung simulieren Sie mit dem Befehlszeilenprogramm Netsh die Konfiguration von DirectAccess-Richtlinien. In der Praxis wird DirectAccess mit Gruppenrichtlinien konfiguriert. Allerdings können sich Situationen ergeben, in denen Sie diese Art von manueller Konfiguration durchführen müssen, zum Beispiel wenn ein Clientcomputer einige Zeit außer Haus war und sich die Adresse des DirectAccess-Servers geändert hat.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an und öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.

2. Geben Sie die folgenden Befehle ein und drücken Sie (nach jeder Zeile) die EINGABETASTE:

```
Netsh interface ipv6 set teredo enterpriseclient 131.107.0.5
Netsh interface 6to4 set relay 131.107.0.5
```

3. Geben Sie nun folgende Diagnosebefehle ein und drücken Sie jeweils die EINGABETASTE. Damit können Sie überprüfen, ob die Konfiguration korrekt durchgeführt wurde. Die IP-Adresse sollte jeweils 131.107.0.5 lauten:

```
Netsh interface 6to4 show relay
Netsh interface ipv6 show teredo
```

Zusammenfassung der Lektion

- DirectAccess ermöglicht einem Client, auf dem Windows 7 Enterprise oder Ultimate ausgeführt wird, ohne Eingreifen des Benutzers eine automatische Verbindung mit dem Intranet einer Organisation, sobald eine aktive Internetverbindung verfügbar ist.
- Wenn ein Windows 7-Client über eine öffentliche IPv6-Adresse verfügt, wird eine direkte IPv6-Verbindung hergestellt. Verfügt der Client über eine öffentliche IPv4-Adresse, wird die Verbindung mit der IP6-zu-IP4-Übergangstechnologie hergestellt. Verfügt der Client über eine private IPv4-Adresse, wird mit der Teredo-Übergangstechnologie eine Verbindung hergestellt. Verfügt der Client über eine private IPv4-Adresse und befindet sich hinter einer Firewall, die die meisten Arten des Netzwerkdatenverkehrs beschränkt, wird die Verbindung mit IP-HTTPS hergestellt.
- DirectAccess-Clients brauchen Computerzertifikate von einer Zertifizierungsstelle, der der DirectAccess-Server vertraut. Der DirectAccess-Server braucht ein Computerzertifikat von einer Zertifizierungsstelle, der die DirectAccess-Clients vertrauen.
- DirectAccess-Clients müssen Mitglieder einer AD DS-Domäne sein. DirectAccess-Clients müssen in der Domäne zudem Mitglieder einer speziellen Sicherheitsgruppe sein, die bei der Einrichtung des DirectAccess-Servers konfiguriert wurde.
- Auf einem DirectAccess-Server muss Windows Server 2008 R2 ausgeführt werden. Außerdem müssen im internen Netzwerk ein Domänencontroller, auf dem Windows Server 2008 R2 ausgeführt wird, und ein DNS-Server vorhanden sein, um DirectAccess zu unterstützen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Verwalten von DirectAccess«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Ein Windows 7-Client ist mit dem Netzwerk eines Hotels verbunden. Clients erhalten in diesem Hotel IP-Adressen aus dem Bereich 10.0.10.0 /24. Die Firewall des Hotels blockiert den Datenverkehr mit Ausnahme der Ports 25, 80 und 443. Mit welcher DirectAccess-Verbindungsmethode kann der Client die Verbindung herstellen?
   A. Teredo
   B. IP6-zu-IP4
   C. Global routbare IPv6-Adresse
   D. IP-HTTPS
2. Sie haben 10 eigenständige Laptops, auf denen Windows 7 Professional verwendet wird. Sie möchten diese Computer so konfigurieren, dass sie mit DirectAccess Zugang zum internen Netzwerk erhalten, wenn Benutzer mit den Laptops in Remotenetzwerken arbeiten. Ihr internes Netzwerk verfügt über eine Domäne, die auf der Funktionsebene Windows Server 2008 R2 arbeitet. Mit welchen der folgenden Schritte erreichen Sie Ihr Ziel? (Wählen Sie alle zutreffenden Antworten.)
   A. Sie aktualisieren die Computer auf Windows 7 Ultimate.
   B. Sie fügen die Computer zur Domäne hinzu.
   C. Sie konfigurieren AppLocker-Richtlinien.
   D. Sie konfigurieren BranchCache-Richtlinien.
3. Welchen der folgenden Computer können Sie als DirectAccess-Server konfigurieren?
   A. Einen Server, auf dem Windows Server 2008 R2 ausgeführt wird und der über zwei Netzwerkkarten verfügt, denen zwei aufeinanderfolgende öffentliche IPv4-Adressen zugewiesen wurden
   B. Einen Server, auf dem Windows Server 2008 R2 ausgeführt wird und der über eine Netzwerkkarte verfügt, der zwei aufeinanderfolgende öffentliche IPv4-Adressen zugewiesen wurde
   C. Einen Server, auf dem Windows Server 2008 R2 ausgeführt wird und der über zwei Netzwerkkarten verfügt, denen eine öffentliche IPv4-Adresse zugewiesen wurde
   D. Einen Server, auf dem Windows Server 2008 R2 ausgeführt wird und der über eine Netzwerkkarte verfügt, der eine öffentliche IPv4-Adresse zugewiesen wurde
4. Kim Akers, die das Benutzerkonto *Kim_Akers* verwendet, hat für eine DirectAccess-Remoteverbindung mit dem internen Netzwerk der Organisation einen Computer namens Laptop-122 verwendet, auf dem Windows 7 Enterprise ausgeführt wird. Laptop-122 ist Mitglied der Domänensicherheitsgruppe *Direct_Access*. Auf Laptop-122 hat sich ein Problem ergeben und Kim hat als Austauschgerät Laptop-123 erhalten, auf dem ebenfalls Windows 7 Enterprise ausgeführt wird und das Mitglied der Domäne *contoso.internal* ist. Wenn Kim remote arbeitet, erhält sie keine Verbindung mit dem internen Netzwerk. Wie lösen Sie dieses Problem?
   A. Sie fügen das Computerkonto von Laptop-123 in der Domäne zur Gruppe *Direct_Access* hinzu.
   B. Sie fügen das Computerkonto von Laptop-123 auf Laptop-123 zur Gruppe *Direct_Access* hinzu.

C. Sie fügen das Benutzerkonto *Kim_Akers* in der Domäne zur Gruppe *Direct_Access* hinzu.

D. Sie fügen das Benutzerkonto *Kim_Akers* auf Laptop-123 zur lokalen Gruppe *Direct_Access* hinzu.

5. Ihr Windows 7-Client ist mit dem Netzwerk eines Hotels verbunden, hat eine Adresse im Netzwerk 192.168.10.0 /24 erhalten und befindet sich hinter einem NAT-Gerät. Das Netzwerk sperrt den ausgehenden Datenverkehr, der nicht über die Ports 80 und 443 erfolgt. Sie möchten überprüfen, ob die IP-HTTPS-Einstellungen für den DirectAccess-Server korrekt sind. Welchen der folgenden Befehle können Sie verwenden?

   A. `ipconfig`

   B. `Netsh interface 6to4 show relay`

   C. `Netsh interface ipv6 show teredo`

   D. `Netsh interface httpstunnel show interfaces`

Lektion 2: Remoteverbindungen

Zwar unterstützt nicht jede Edition von Windows 7 DirectAccess, aber jede Edition von Windows 7 unterstützt VPN mit den Protokollen PPTP, L2TP/IPsec, SSTP und IKEv2. Die herkömmliche VPN-Technologie ist wichtig, weil sie mit Ausnahme von IKEv2 zu den gebräuchlichen Remotezugriffsinfrastrukturen kompatibel ist und nicht voraussetzt, dass eine Organisation Server auf Windows Server 2008 R2 aktualisiert. Zudem sind PPTP- und L2TP/IPsec-VPNs zu Remotezugriffslösungen von anderen Herstellern kompatibel. Das ist wichtig, wenn Ihre Organisation nicht die Remotezugriffsinfrastruktur von Windows Server einsetzt. In dieser Lektion erfahren Sie, wie man mit Clients umgeht, die der NAP-Quarantäne unterliegen, und wie man einen Remotedesktopclient so konfiguriert, dass er ohne VPN-Verbindung auf Remotedesktopdiensteserver aus dem geschützten internen Netzwerk zugreifen kann.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Herstellen von VPN-Verbindungen
- Konfigurieren der VPN-Authentifizierung
- Einrichten von VPN-Reconnect
- Verwalten der VPN-Sicherheitsüberwachung
- Konfigurieren der Wartung für in NAP-Quarantäne befindliche Computer

Veranschlagte Zeit für diese Lektion: 40 Minuten

Virtuelle private Netzwerke

VPNs ermöglichen über das Internet die Verbindung von Computern mit Remotenetzwerken. VPN-Benutzer können auf Ressourcen aus dem LAN zugreifen, wie E-Mail, freigegebene Ordner, Drucker, Datenbanken und Terminplaner, während sie mit ihren Computern irgendwo außerhalb des Büros arbeiten. Um ein VPN verwenden zu können, brauchen sie nur eine aktive Internetverbindung und die erforderliche VPN-Infrastruktur in dem Netzwerk, mit dem sie eine Verbindung herstellen. Die Einrichtung von VPNs bedeutet, dass Ressourcen aus den geschützten Netzwerken der Organisation für autorisierte Internetbenutzer verfügbar gemacht werden können, ohne dass diese Ressourcen für andere Internetbenutzer zugänglich werden. VPNs sind wie Tunnel, die bestimmten autorisierten Benutzern aus dem Internet Zugang zu den konfigurierten internen Netzwerkressourcen ermöglichen. Benutzer ohne Administratorrechte können Remotezugriffsverbindungen einrichten. Mit den Gruppenrichtlinien im Knoten *Benutzerkonfiguration\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen* können die Benutzerrechte zur Erstellung und Änderung von Remotezugriffsverbindungen eingeschränkt werden.

Bei der Erstellung einer VPN-Verbindung müssen Sie die Adresse des VPN-Servers angeben, mit dem eine Verbindung hergestellt werden soll, sowie die Anmeldeinformationen für die Authentifizierung. Sie können eine neue VPN-Verbindung im Netzwerk- und Freigabecenter einrichten. Dazu klicken Sie auf *Neue Verbindung oder neues Netzwerk einrichten* und dann auf *Verbindung mit dem Arbeitsplatz herstellen*. Wenn Sie eine neue VPN-Verbindung erstellen, stellt Windows 7 den VPN-Typ auf *Automatisch*. Sie können eine Verbindung zwar so einstellen, dass ein bestimmtes VPN-Protokoll verwendet wird, aber dann probiert Windows 7 die anderen VPN-Protokolle nicht aus, wenn das von Ihnen gewählte Protokoll nicht

anwendbar ist. In den Übungen am Ende dieser Lektion erstellen Sie eine VPN-Verbindung und stellen im Eigenschaftendialogfeld der Verbindung ein bestimmtes Protokoll ein.

Wenn der Typ einer VPN-Verbindung auf *Automatisch* gestellt ist, versucht Windows 7 zuerst, mit dem sichersten Protokoll eine Verbindung herzustellen. Windows 7-Computer können vier verschiedene VPN-Protokolle verwenden, die sich in der Verschlüsselungsart und in ihrer Fähigkeit unterscheiden, die Daten zu schützen. Die sichersten Protokolle bieten:

- **Datenvertraulichkeit (Verschlüsselung)** Das Protokoll verschlüsselt Ihre Daten, damit andere nicht mitlesen können, wenn die Daten durch öffentliche Netzwerke laufen.
- **Datenintegrität** Sie erfahren es, wenn Ihre Daten während der Übertragung verändert wurden.
- **Schutz vor Wiedergabeangriffen** Dieselben Daten können nur einmal gesendet werden. Bei einem Wiedergabeangriff würde ein Angreifer die Daten abfangen und anschließend erneut senden.
- **Datenursprungsauthentifizierung** Absender und Empfänger können sich der Identität des Kommunikationspartners sicher sein.

Windows 7 unterstützt folgende VPN-Protokolle, sortiert nach steigender Sicherheit:

- **PPTP** PPTP-VPNs sind die unsicherste VPN-Form. Da PPTP-VPNs keine Public Key-Infrastruktur (PKI) erfordern, sind sie zudem die verbreitetste VPN-Form. PPTP-Verbindungen können die Authentifizierungsprotokolle MS-CHAP, MS-CHAPv2, EAP und PEAP verwenden. Zur Verschlüsselung der PPTP-Daten verwenden PPTP-Verbindungen MPPE. PPTP-Verbindungen bieten Datenvertraulichkeit, aber keine Datenintegrität oder Datenursprungsauthentifizierung. Einige ältere NAT-Geräte unterstützen PPTP nicht. Windows 7 verwendet PPTP zur Unterstützung eingehender VPN-Verbindungen. Die Konfiguration von Windows 7 zur Unterstützung eingehender VPN-Verbindungen wird im Verlauf dieser Lektion noch ausführlicher beschrieben.
- **L2TP/IPsec** L2TP/IPsec-VPN-Verbindungen sind sicherer als PPTP. L2TP/IPsec bietet auf Paketbasis Datenursprungsauthentifizierung, Datenintegrität, Schutz vor Wiedergabeangriffen und Datenvertraulichkeit. L2TP/IPsec verwendet digitale Zertifikate, erfordert also Zugang zu einer Zertifikatdiensteinfrastruktur. Die meisten VPN-Lösungen auf dem Markt unterstützen L2TP/IPsec. L2TP/IPsec kann nicht hinter NAT verwendet werden, wenn Client und Server kein IPsec NAT Traversal (NAT-T) unterstützen. Windows 7, Windows Server 2003 und Windows Server 2008 unterstützen NAT-T. In den erweiterten Eigenschaften können Sie einstellen, ob L2TP die Authentifizierung mit einem vordefinierten Schlüssel oder mit Zertifikaten durchführt (Abbildung 10.11).
- **SSTP** SSTP-VPN-Tunnel verwenden Port 443. Das bedeutet, dass der SSTP-VPN-Datenverkehr die meisten Firewalls durchlaufen kann, die Internetzugang zulassen. Für die VPN-Protokolle PPTP, L2TP/IPsec und IKEv2 gilt das nicht. SSTP kapselt den PPP-Datenverkehr über den SSL-Kanal des HTTPS-Protokolls. SSTP unterstützt Datenursprungsauthentifizierung, Datenintegrität, Schutz vor Wiedergabeangriffen (replay) und Datenvertraulichkeit. Sie können SSTP nicht über einen Webproxy verwenden, der eine Authentifizierung verlangt.

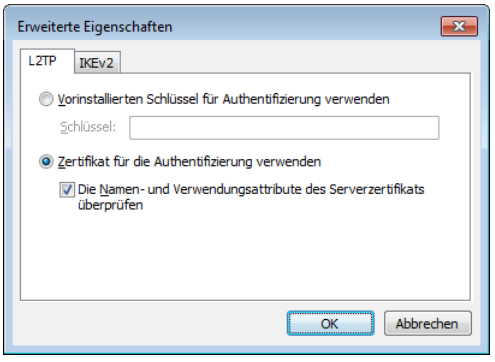


Abbildung 10.11 Erweiterte Eigenschaften für L2TP

- **IKEv2** IKEv2 ist ein neues VPN-Protokoll von Windows 7. In älteren Windows-Versionen ist es nicht verfügbar. IKEv2 unterstützt IPv6 und die neue Funktion VPN-Reconnect. Zur clientseitigen Authentifizierung unterstützt IKEv2 EAP (Extensible Application Protocol) und Computerzertifikate. Verfügbar sind die Einstellungen *Microsoft: Geschütztes EAP (PEAP)*, *Microsoft: Gesichertes Kennwort (EAP-MS-CHAP v2)* und *Microsoft: Smartcard oder anderes Zertifikat* (Abbildung 10.12). IKEv2 unterstützt nicht POP, CHAP oder MS-CHAPv2 (ohne EAP) als Authentifizierungsprotokolle. IKEv2 unterstützt Datenursprungsauthentifizierung, Datenintegrität, Schutz vor Wiedergabeangriffen und Datenvertraulichkeit. IKEv2 verwendet UDP-Port 500. Wenn Sie unter Windows 7 eine neue VPN-Verbindung mit den Standardeinstellungen konfigurieren, versucht Windows 7 zuerst, eine IKEv2-Verbindung herzustellen.

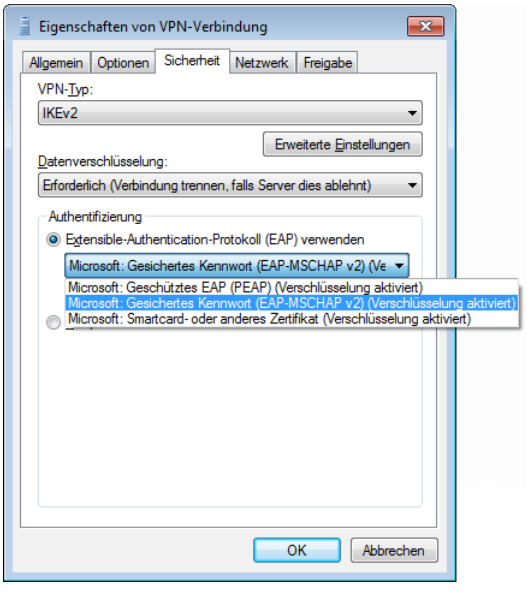


Abbildung 10.12 Von IKEv2 unterstützte Authentifizierungsprotokolle

VPN-Authentifizierungsprotokolle

Windows 7 unterstützt für Einwähl- und VPN-Verbindungen verschiedene Authentifizierungsprotokolle. Authentifizierungsprotokolle lassen sich in zwei Kategorien aufteilen: Authentifizierungsprotokolle auf Kennwortbasis und Authentifizierungsprotokolle auf Zertifikatbasis. Authentifizierungsprotokolle auf Zertifikatbasis erfordern die Bereitstellung einer PKI-Lösung wie die Active Directory-Zertifikatdienste. Wenn Sie ein Authentifizierungsprotokoll auf Zertifikatbasis verwenden, müssen Sie Zertifikate bereitstellen, die an Benutzerkonten, an Computerkonten oder an beide Kontenarten gebunden sind. Die Eigenschaften dieser Protokolle sind wie folgt:

- **PAP (Password Authentication Protocol)** Dieses Protokoll verwendet zur Authentifizierung unverschlüsselte Kennwörter. Für VPN-Verbindungen ist es unter Windows 7 standardmäßig nicht aktiviert und wird auch nicht von Remotezugriffsservern unterstützt, auf denen Windows Server 2008 verwendet wird. Dieses Protokoll würden Sie nur aktivieren, um eine Verbindung mit einem älteren VPN-Server herzustellen, der keine sichereren Protokolle unterstützt.
- **CHAP (Challenge Authentication Protocol)** Dies ist ein Authentifizierungsprotokoll auf Kennwortbasis. Obwohl Remotezugriffsserver, auf denen Windows Server 2008 ausgeführt wird, dieses Protokoll nicht unterstützen, wird es unter Windows 7 standardmäßig für VPN-Verbindungen aktiviert und ermöglicht eine Verbindung mit VPN-Servern, die keine sichereren Protokolle unterstützen.

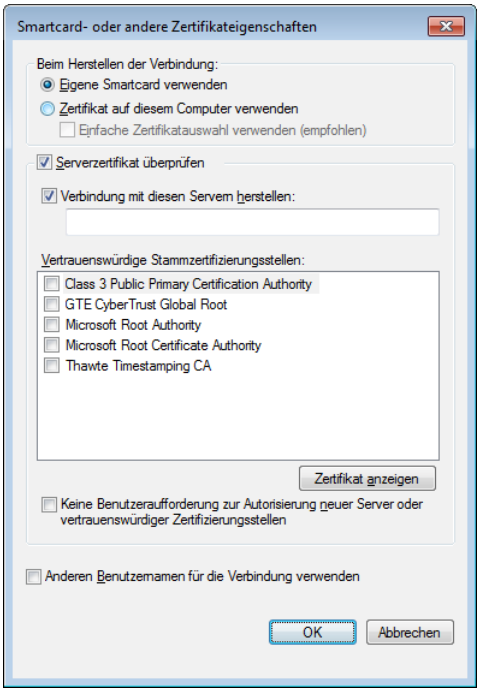


Abbildung 10.13 Optionen für Smartcards oder andere Zertifikate

- **MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2)** MS-CHAPv2 ist ein Authentifizierungsprotokoll auf Kennwortbasis. Sie können eine VPN-Verbindung konfigurieren, die dieses Protokoll und zur Authentifizierung die Anmeldeinformationen des aktuell angemeldeten Benutzers verwendet.
- **PEAP/PEAP-TLS (Protected Extensible Authentication Protocol with Transport Layer Security)** Dies ist ein Authentifizierungsprotokoll auf Zertifikatbasis, bei dem sich die Benutzer mit Zertifikaten authentifizieren. Erfordert die Installation eines Computerzertifikats auf dem VPN-Server.
- **EAP-MS-CHAPv2/PEAP-MS-CHAPv2** Das sicherste Authentifizierungsprotokoll auf Kennwortbasis, das unter Windows 7 für VPN-Clients verfügbar ist. Erfordert die Installation eines Computerzertifikats auf dem VPN-Server. Erfordert kein Clientzertifikat.
- **Smartcard- oder anderes Zertifikat** Verwenden Sie dieses Protokoll, wenn Benutzer VPN-Verbindungen mit einer Smartcard oder einem Zertifikat authentifizieren, das auf dem Computer installiert ist. Abbildung 10.13 zeigt das Eigenschaftendialogfeld für dieses Authentifizierungsprotokoll.

Im Eigenschaftendialogfeld einer VPN-Verbindung, das sich auf der Seite *Netzwerkverbindungen* der Systemsteuerung öffnen lässt, können Sie festlegen, welche VPN-Authentifizierungsprotokolle für die Verbindung zulässig sind (Abbildung 10.14). Windows probiert zuerst das sicherste aktivierte Authentifizierungsprotokoll und versucht bei Bedarf dann, mit den weniger sicheren verfügbaren Protokollen eine Verbindung herzustellen.

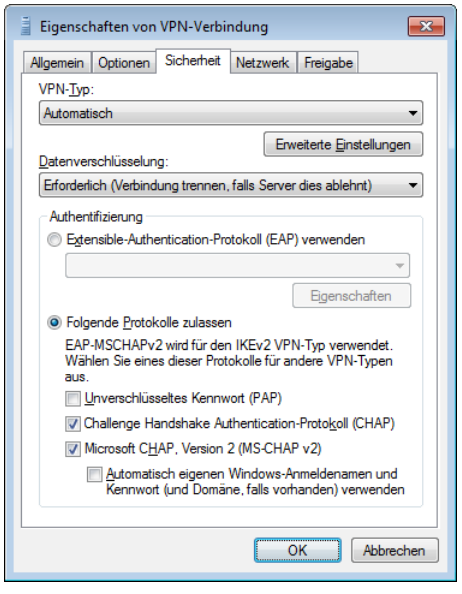


Abbildung 10.14 VPN-Authentifizierungsprotokolle

VPN-Reconnect

VPN-Reconnect ist eine neue Funktion von Windows 7. Wenn Sie mit den Protokollen PPTP, L2TP/IPsec oder SSTP eine Verbindung mit einem VPN-Server herstellen und es zu einer Störung im Netzwerk kommt, können Sie die VPN-Verbindung verlieren und müssen sie erneut herstellen. Geschieht dies bei der Übertragung einer Datei, beim Herunterladen von E-Mail oder beim Versenden eines Druckauftrags, müssen Sie wieder von vorne anfangen. VPN-Reconnect ermöglicht Windows 7-Computern eine automatische Wiederherstellung der Verbindung, selbst wenn die Unterbrechung bereits 8 Stunden dauert. VPN-Reconnect funktioniert auch dann, wenn die Unterbrechung durch den Wechsel auf einen neuen Internetzugriffspunkt hervorgerufen wurde. Vielleicht verwendet ein Benutzer zum Beispiel eine VPN-Verbindung mit dem Firmennetzwerk, während er auf einem Flughafen in einem Café wartet und mit dessen Drahtlosnetzwerk verbunden ist. Wenn sich der Zeitpunkt des Abflugs nähert, geht er vom Café in die Wartehalle des Flughafens, die über ihr eigenes Wi-Fi-Netzwerk verfügt. VPN-Reconnect sorgt dafür, dass die VPN-Verbindung des Benutzers automatisch wiederhergestellt wird, sobald der Benutzer im neuen Netzwerk über eine Internetverbindung verfügt. Bei einer herkömmlichen VPN-Lösung müsste er die Verbindung manuell wieder herstellen, wenn er im neuen Drahtlosnetzwerk der Wartehalle über eine Internetverbindung verfügt, und die aktuellen Vorgänge, die über das VPN abgewickelt wurden, wären verloren. Im Gegensatz zu DirectAccess, das nur in einigen Editionen von Windows 7 unterstützt wird, unterstützen alle Editionen von Windows 7 VPN-Reconnect.

VPN-Reconnect verwendet das IKEv2-Tunnelprotokoll mit der MOBIKE-Erweiterung. Die MOBIKE-Erweiterung ermöglicht es VPN-Clients, ihre Internetadressen zu ändern, ohne eine erneute Authentifizierung beim VPN-Server durchführen zu müssen. Nur VPN-Server unter Windows Server 2008 R2 unterstützen IKEv2. Sie können IKEv2 nicht einsetzen, wenn Ihre Organisation einen Routing- und RAS-Server unter Windows Server 2003, Windows Server 2003 R2 oder Windows Server 2008 verwendet.

Sie können für VPN-Reconnect eine Netzwerkausfallzeit von maximal 8 Stunden einstellen (Abbildung 10.15). Nach Ablauf der eingestellten Netzwerkausfallzeit ist es erforderlich, die Verbindung manuell wiederherzustellen. In der Übung am Ende dieser Lektion erstellen und konfigurieren Sie eine VPN-Verbindung auf IKEv2-Basis.

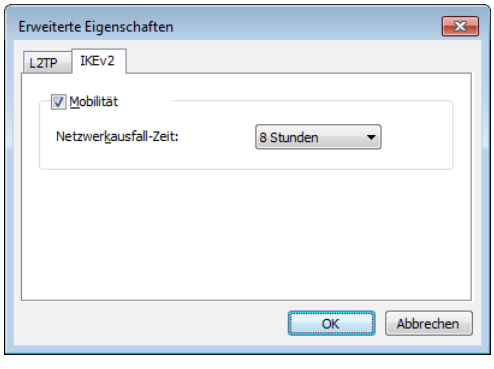


Abbildung 10.15 Erweiterte IKEv2-Eigenschaften

Schnelltest

- Welches VPN-Protokoll unterstützt die automatische Wiederverbindung?

Antwort zum Schnelltest

- IKEv2 unterstützt die automatische Wiederverbindung.

NAP-Wartung

Der Netzwerkzugriffsschutz (Network Access Protection, NAP) ist eine Technologie von Windows Server 2008, die den Netzwerkzugang auf der Basis einer Integritätseinstufung des Clients einschränken kann. Ein konformer Client, der alle Integritätsanforderungen erfüllt, erhält Zugang zum Netzwerk. Erfüllt er die Voraussetzungen nicht, ist er nicht konform. NAP hindert nichtkonforme Clients am Zugang zum Netzwerk. NAP kann für Clients verwendet werden, die direkt am LAN angeschlossen sind, aber auch für VNP-, Remotedesktopgateway- und DirectAccess-Clients. Administratoren können NAP so konfigurieren, dass der Zugang zum Netzwerk auf der Basis folgender Kriterien eingeschränkt wird:

- Ist auf dem Client Antivirensoftware installiert und ist sie auf dem neusten Stand?
- Ist auf dem Client Antispysoftware installiert und ist sie auf dem neusten Stand?
- Ist auf dem Client die Windows-Firewall aktiviert?
- Ist die Funktion Automatische Updates aktiviert?
- Sind alle Softwareupdates auf dem Client installiert?

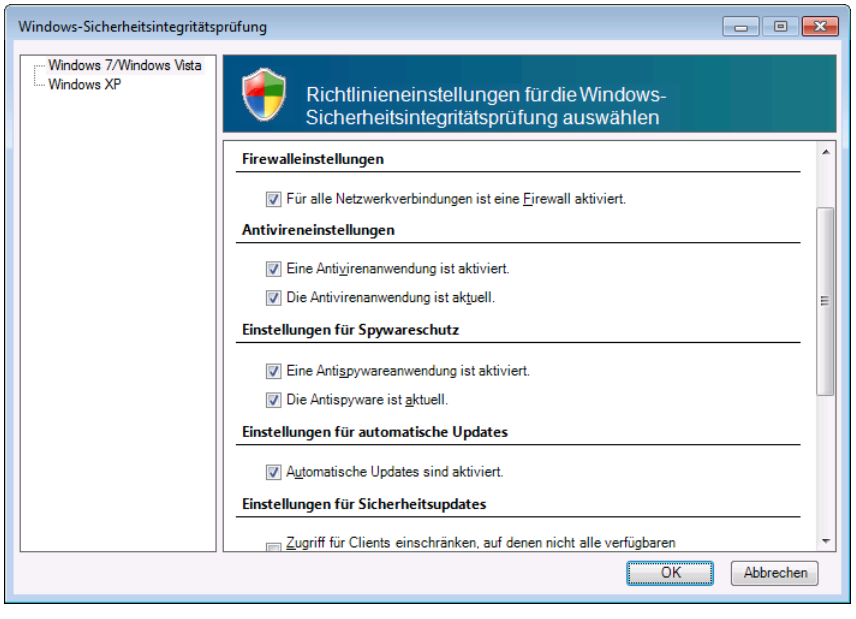


Abbildung 10.16 Windows-Sicherheitsintegritätsprüfung

Administratoren geben diese Kriterien in der Systemintegritätsprüfung ein (Security Health Validator, SHV). Administratoren können einstellen, welche Komponenten in der Systemintegritätsprüfung berücksichtigt werden. Abbildung 10.16 zeigt die Windows 7-Systemintegritätsprüfung von Windows Server 2008 R2.

Administratoren können NAP so einstellen, dass Clients, die nicht die Integritätsanforderungen erfüllen, gewartet werden. Wird NAP auf VPN-Verbindungen angewendet, bedeutet dies häufig die Bereitstellung eines geeigneten Wartungsnetzwerks. Ein Wartungsnetzwerk ist ein spezielles Netzwerk, das Dienstleistungen anbietet, mit denen der Client wieder in einen konformen Zustand gebracht werden kann. Nichtkonforme Clients können zwar mit Hosts aus dem Wartungsnetzwerk kommunizieren, aber nicht mit Hosts aus dem internen Netzwerk der Organisation. Ein Wartungsnetzwerk kann einen WSUS-Server (Windows Software Update Services) enthalten, damit der Client die neusten Softwareupdates erhält, und einen Antivirus-Updateserver, damit auch die Schutzsoftware des Clients den Integritätsanforderungen genügt und er Zugang zum internen Netzwerk erhält.

Ein Windows 7-Client kann einige Wartungsschritte automatisch durchführen, wenn der Dienst *Sicherheitscenter* aktiviert ist. Dieser Dienst arbeitet mit dem Wartungscenter von Windows 7 zusammen. Wenn dieser Dienst aktiviert ist und in der Remotezugriffsinfrastruktur die entsprechenden NAP-Richtlinien konfiguriert sind, können sich Clients automatisch in einen konformen Zustand versetzen, indem sie die Windows-Firewall aktivieren, Windows Update ausführen und die Antiviren- und Antispyware-Software aktualisieren.

In Umgebungen ohne Wartungsnetzwerke ist es erforderlich, dass Benutzer ihre Computer manuell in einen konformen Zustand versetzen, damit sie eine Remotezugriffsverbindung herstellen können. Wenn Ihre Organisation in ihrer Remotezugriffsinfrastruktur NAP verwendet, sollten Sie dafür sorgen, dass die Benutzer wissen, was zu tun ist, damit ihre Windows 7-Clients konform werden und Zugang zum internen Netzwerk erhalten.



Weitere Informationen NAP

Im NAP TechCenter unter *http://technet.microsoft.com/en-us/network/bb545879.aspx* erfahren Sie mehr über den Netzwerkzugriffsschutz.

Remotedesktop und die Veröffentlichung von Anwendungen

Die Remotedesktopdienste von Windows Server 2008 R2 (unter Windows Server 2008 und Windows Server 2003 noch Terminaldienste genannt) ermöglichen den Benutzern die Herstellung einer Remotedesktopverbindung von einem Client zu einem Server, auf dem sie Anwendungen ausführen können. Wie unter Windows 7 Remotedesktopverbindungen zu Clients erstellt werden, haben Sie bereits in Kapitel 7, »Windows-Firewall und Remoteverwaltung«, erfahren.

Das Remotedesktopgateway (früher Terminaldienstegateway) ermöglicht Internetbenutzern die Erstellung von Remotedesktopverbindungen mit Servern aus einem internen Netzwerk, ohne eine VPN-Verbindung einrichten zu müssen. Verbindungen können nur zu speziell konfigurierten Remotedesktophosts aus dem internen Netzwerk hergestellt werden. Benutzer haben wie beim herkömmlichen VPN oder DirectAccess keinen Zugang zu allen Netzwerkressourcen.



Weitere Informationen Remotedesktopgateway

Weitere Informationen über das Remotedesktopgateway finden Sie in folgendem Microsoft TechNet-Artikel: *http://technet.microsoft.com/en-us/library/dd560672.aspx.*

Um über einen Remotedesktop-Gatewayserver eine Verbindung herzustellen, wechseln Sie im Dialogfeld *Remotedesktopverbindung* auf die Registerkarte *Erweitert* und klicken unter *Verbindung von überall aus herstellen* auf *Einstellungen*. Dadurch öffnet sich das Dialogfeld *Remotedesktop-Gatewayservereinstellungen*. In diesem Dialogfeld können Sie Einstellungen für das Remotedesktopgateway vornehmen und zum Beispiel festlegen, ob das Remotedesktopgateway automatisch ermittelt werden soll oder ob Sie einen bestimmten Remotedesktop-Gatewayserver verwenden möchten, wie in Abbildung 10.17. Sie können auch die Option *Keinen Remotedesktop-Gatewayserver verwenden* wählen.

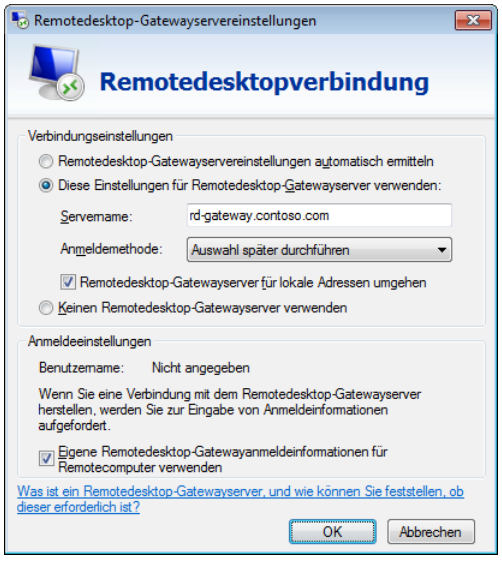


Abbildung 10.17 Remotedesktop-Gatewayservereinstellungen

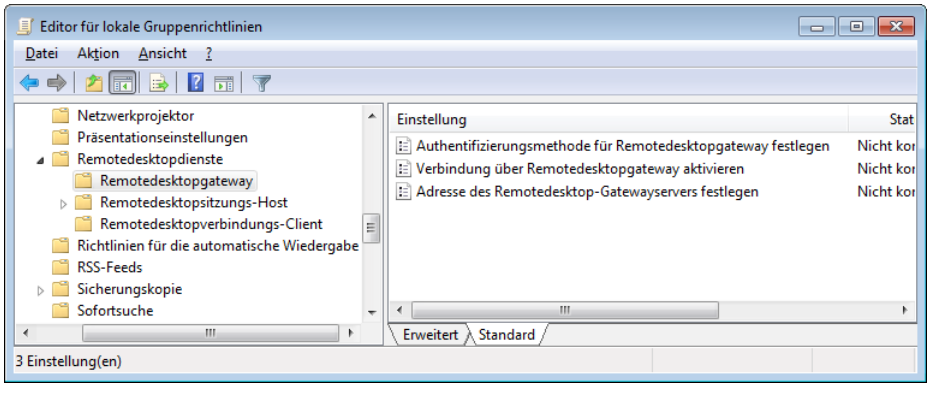


Abbildung 10.18 Richtlinien für das Remotedesktopgateway

Sie können die Konfiguration des Remotedesktopgateways auch in Gruppenrichtlinien durchführen, statt die Einstellungen manuell vorzunehmen. Die entsprechenden Richtlinien liegen im Knoten *Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remotedesktopgateway* (Abbildung 10.18).

Diese Richtlinien funktionieren wie folgt:

- **Authentifizierungsmethode für Remotedesktopgateway festlegen** Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird die Authentifizierungsmethode verwendet, die der Benutzer angibt. Wird die Richtlinie aktiviert, kann der Administrator eine Änderung der Einstellung durch den Benutzer zulassen und unter folgenden Optionen wählen:
  - *Anmeldeinformationen anfordern, NTLM-Protokoll verwenden*
  - *Anmeldeinformationen anfordern, Standardprotokoll verwenden*
  - *Lokale Anmeldeinformationen verwenden*
  - *Smartcard verwenden*
- **Verbindung über Remotedesktopgateway aktivieren** Wenn diese Richtlinie aktiviert ist, versucht der Remotedesktopclient automatisch, eine Verbindung über das konfigurierte Remotedesktopgateway herzustellen, wenn er keine Verbindung mit dem konfigurierten Remotedesktopdiensteserver herstellen kann. Diese Richtlinie lässt sich nur erzwingen, wenn die Richtlinie *Adresse des Remotedesktop-Gatewayservers festlegen* konfiguriert ist. Die Richtlinie lässt sich mit einer Option so einstellen, dass Benutzer die Einstellung ändern können.
- **Adresse des Remotedesktop-Gatewayservers festlegen** Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, versuchen Clients automatisch zu erkennen, ob ein Remotedesktopgateway erforderlich ist. Ist dies der Fall, wird das Remotedesktopgateway verwendet, das der Benutzer angibt. Wenn die Richtlinie aktiviert ist, wird die in der Richtlinie angegebene Adresse des Remotedesktop-Gatewayservers verwendet. Die Adresse des Remotedesktop-Gatewayservers muss zu dem SSL-Zertifikat passen, das auf dem Remotedesktop-Gatewayserver installiert ist.

RemoteApp ermöglicht es Anwendungen, die auf Remotedesktopdiensteservern ausgeführt werden, ihre Bildschirmausgabe auf den Remotedesktopclients anzuzeigen. Darin unterscheidet sich RemoteApp von einer Standardsitzung mit Remotedesktopverbindung, bei der der Benutzer den gesamten Desktop in einem Fenster sieht. Wenn Sie zum Beispiel die Anwendung Microsoft Office Excel 2007 mit RemoteApp veröffentlichen und ein Benutzer diese Anwendung verwendet, sieht er ein ganz normales Excel 2007-Anwendungsfenster, als würde er die Anwendung lokal ausführen. RemoteApp-Anwendungen werden zudem wie andere lokal installierte Anwendungen im *Start*-Menü angezeigt. Der Unterschied besteht darin, dass die RemoteApp-Anwendung auf dem Remotedesktopdiensteserver ausgeführt wird, während nur die Bildschirmausgaben der Anwendung auf dem Client angezeigt werden.

Sie können RemoteApp-Anwendungen auch über das Internet verwenden, wenn die Verknüpfung mit der RemoteApp-Anwendung oder die RemoteApp-Veröffentlichung die Adresse eines Remotedesktop-Gatewayservers enthält. Die Adresse des Remotedesktop-Gatewayservers legen Sie vor der Veröffentlichung von Anwendungen im Dialogfeld *Einstellungen für die RemoteApp-Bereitstellung* fest (Abbildung 10.19). Dieses Dialogfeld ist auf einem Computer, auf dem Windows Server 2008 R2 ausgeführt wird, über den Remote-

App-Manager zugänglich. Wenn Sie eine RemoteApp-Anwendung über Gruppenrichtlinien oder durch Verteilung einer Remotedesktop-Verknüpfungsdatei (*.rdp*) veröffentlichen, bevor Sie ein Remotedesktopgateway konfigurieren, müssen Sie die Anwendung erneut veröffentlichen und die Datei erneut verteilen.

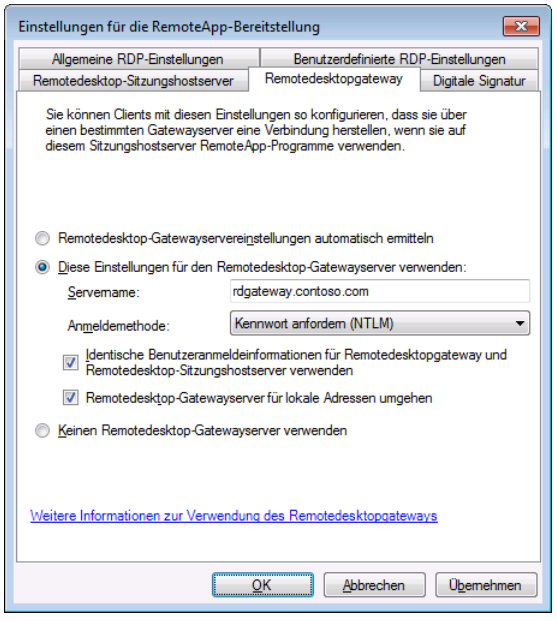


Abbildung 10.19 Remotedesktopgatewayeinstellungen für RemoteApp



Weitere Informationen RemoteApp

Weitere Informationen über RemoteApp erhalten Sie auf der folgenden Microsoft TechNet-Webseite: *http://technet.microsoft.com/de-de/library/cc755055.aspx.*

Einwählverbindungen

Viele Leute verwenden auch heute noch Einwählverbindungen, um eine Internetverbindung herzustellen. Windows 7 unterstützt Einwählverbindungen mit Internetanbietern, sofern ein kompatibles Modem verfügbar ist. Modems gibt es in unterschiedlichen Bauformen, beispielsweise als herkömmliches verkabeltes externes Gerät, Funkmodem, in die Hardware des portablen Computers integriert, oder als aufsteckbares USB-Gerät.

So richten Sie eine Wählverbindung ein:

1. Klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Wählen Sie auf der Seite *Wählen Sie eine Verbindungsoption aus* die Option *Wählverbindung einrichten* (Abbildung 10.20) und klicken Sie dann auf *Weiter*.
2. Geben Sie im Dialogfeld *Wählverbindung erstellen* die Telefonnummer des Internetanbieters ein, Ihren Benutzernamen beim Internetanbieter, das Kennwort und einen Namen für die Verbindung (Abbildung 10.21). Legen Sie außerdem fest, ob andere Benutzer des Computers diese Verbindung verwenden dürfen.

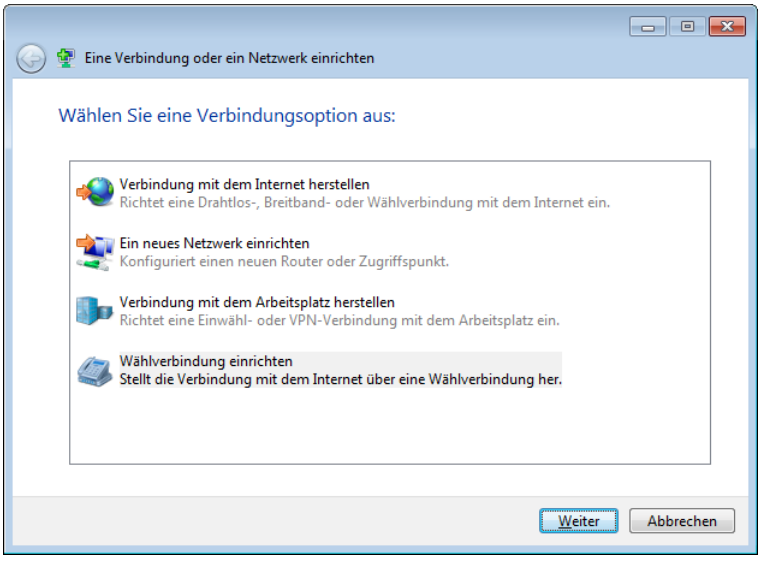

Eine Verbindung oder ein Netzwerk einrichten
Wählen Sie eine Verbindungsoption aus:
Verbindung mit dem Internet herstellen
Richtet eine Drahtlos-, Breitband- oder Wählverbindung mit dem Internet ein.
Ein neues Netzwerk einrichten
Konfiguriert einen neuen Router oder Zugriffspunkt.
Verbindung mit dem Arbeitsplatz herstellen
Richtet eine Einwähl- oder VPN-Verbindung mit dem Arbeitsplatz ein.
Wählverbindung einrichten
Stellt die Verbindung mit dem Internet über eine Wählverbindung her.
Weiter
Abbrechen

Abbildung 10.20 Einrichten einer Wählverbindung

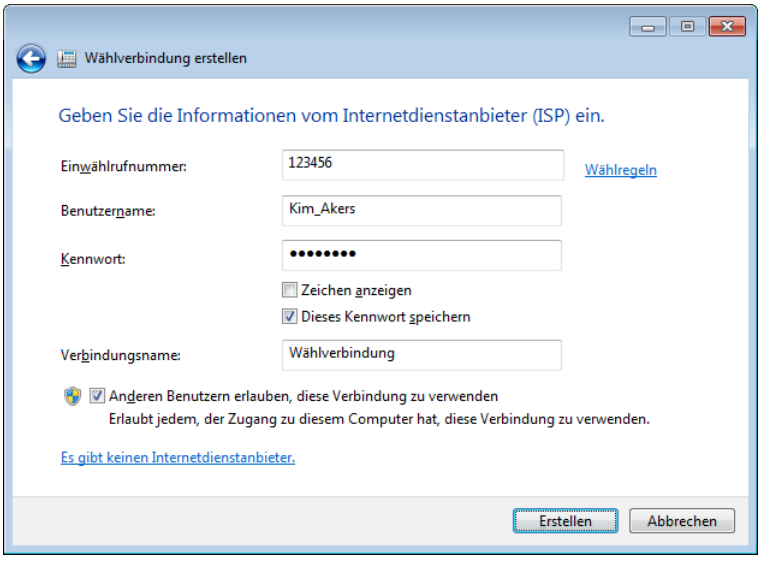


Abbildung 10.21 Festlegen der Verbindungsdaten

3. Wenn Sie noch Regeln für das Wählen festlegen müssen, beispielsweise eine Ortskennzahl, eine Netzkennzahl, eine Amtskennziffer, oder wenn Sie festlegen wollen, ob eine Ton- oder Impulswahl erfolgt, können Sie auf *Wählregeln* klicken und diese Einstellungen vornehmen.

Konfigurieren von Windows 7 für die Annahme von eingehenden Verbindungen

Sie können Windows 7 so konfigurieren, dass es eingehende VPN- und Einwählverbindungen akzeptiert. In diesem Fall dient Windows 7 als VPN- und Einwählserver. Windows 7 unterstützt eingehende VPN-Verbindungen mit dem PPTP-Protokoll und lässt zu jedem Zeitpunkt immer nur eine eingehende Verbindung zu. So konfigurieren Sie Windows 7 für die Unterstützung eingehender Verbindungen:

1. Öffnen Sie die Seite *Netzwerkverbindungen*, die im Netzwerk- und Freigabecenter durch Klick auf *Adaptereinstellungen ändern* zugänglich ist. Drücken Sie auf die ALT-Taste, damit die Menüleiste sichtbar wird. Klicken Sie auf *Datei* und dann auf *Neue eingehende Verbindung*.
2. Wählen Sie die Benutzer aus, die per VPN- oder Wählverbindung Remotezugriff auf den Computer erhalten sollen, und klicken Sie dann auf *Weiter* (Abbildung 10.22).

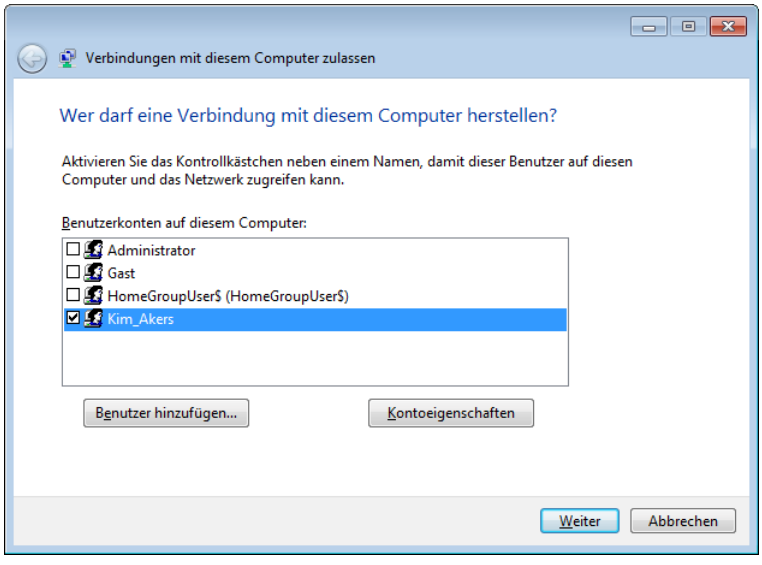


Abbildung 10.22 Auswählen der Remotebenutzer

3. Wählen Sie auf der Seite *Wie stellen die Benutzer eine Verbindung her?* die Verbindungsarten aus, die unterstützt werden sollen. Verfügbar sind die Optionen *Über das Internet* und *Über ein Modem*.
4. Wählen Sie auf der Seite *Die Netzwerksoftware ermöglicht dem Computer das Annehmen von Verbindungen von anderen Computern* die Netzwerkkomponenten aus, die für eingehende Verbindungen aktiviert werden. Standardmäßig werden IPv4 und die Datei- und Druckerfreigabe aktiviert. IPv6 ist standardmäßig deaktiviert.
5. Durch einen Klick auf *Eigenschaften* können Sie für IPv4 festlegen, wie der Client seine Adresse erhält (Abbildung 10.24). Zur Wahl stehen die automatische Zuweisung über DHCP (Dynamic Host Configuration Protocol), eine Adresse aus einem IP-Adressenpool oder die Angabe einer eigenen IP-Adresse durch den Client.

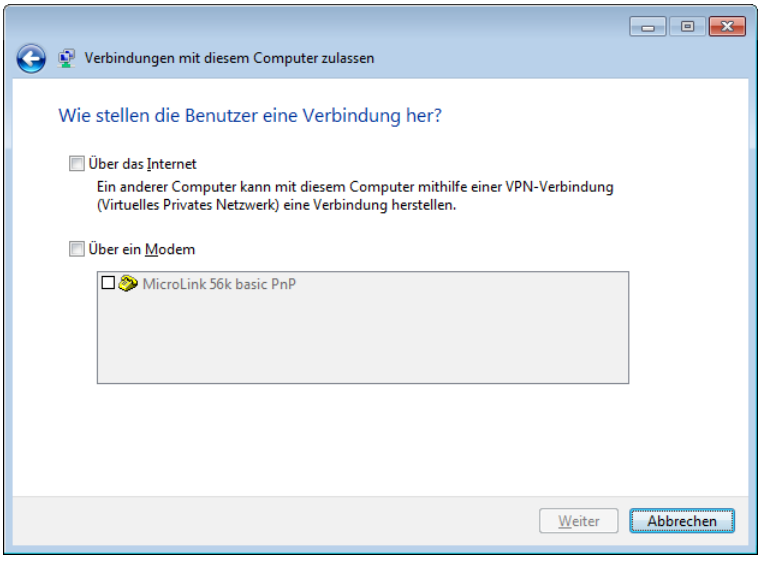

Verbindungen mit diesem Computer zulassen
Wie stellen die Benutzer eine Verbindung her?
Über das Internet
Ein anderer Computer kann mit diesem Computer mithilfe einer VPN-Verbindung (Virtuelles Privates Netzwerk) eine Verbindung herstellen.
Über ein Modem
MicroLink 56k basic PnP
Weiter
Abbrechen

Abbildung 10.23 Konfigurieren der eingehenden Verbindung

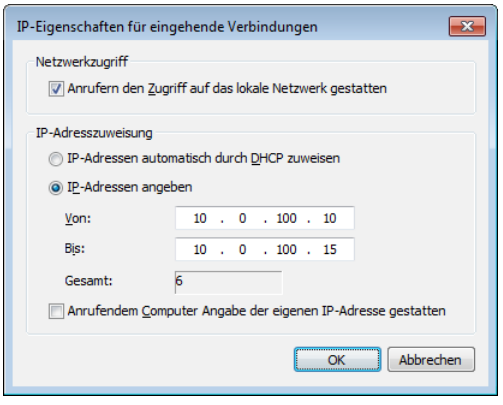

IP-Eigenschaften für eingehende Verbindungen
Netzwerkzugriff
Anrufern den Zugriff auf das lokale Netzwerk gestatten
IP-Adresszuweisung
IP-Adressen automatisch durch DHCP zuweisen
IP-Adressen angeben
Von: 10 . 0 . 100 . 10
Bis: 10 . 0 . 100 . 15
Gesamt: 6
Anrufendem Computer Angabe der eigenen IP-Adresse gestatten
OK
Abbrechen

Abbildung 10.24 Eigenschaften eingehender Verbindungen

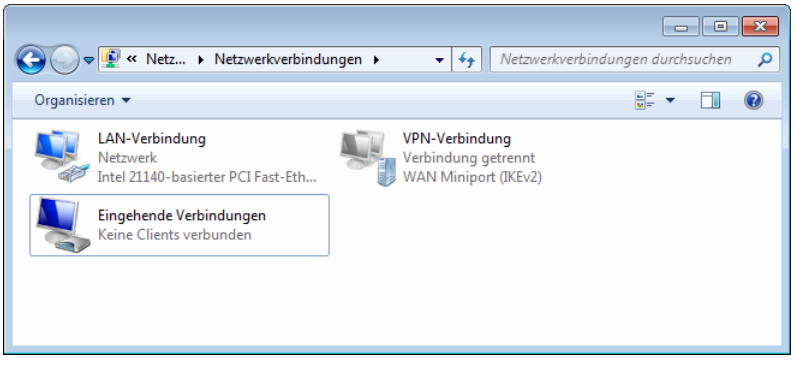


Abbildung 10.25 Die eingehenden Verbindungen wurden konfiguriert

6. Klicken Sie auf *Zugriff zulassen*. Auf der Seite *Netzwerkverbindungen* gibt es anschließend ein neues Element namens *Eingehende Verbindungen* (Abbildung 10.25). Im Eigenschaftendialogfeld dieses Elements können Sie festlegen, welche Benutzer eingehende Verbindungen herstellen dürfen. Um dieses Dialogfeld zu öffnen, klicken Sie das Element *Eingehende Verbindungen* mit der rechten Maustaste an und wählen *Eigenschaften*.

Überwachung von Remoteverbindungen

Wenn Sie Windows 7 für eingehende VPN- oder Einwählverbindungen konfigurieren, werden Sie diese Verbindungen überwachen wollen. Damit erhalten Sie Informationen darüber, welche Benutzer eine Remoteverbindung mit dem Windows 7-Client hergestellt haben. Zur einfachen Überwachung sollten Sie die Richtlinie *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie\Anmeldeereignisse überwachen* aktivieren. Dann werden alle An- und Abmeldeversuche auf dem Computer überwacht, für den die Richtlinie wirksam ist.

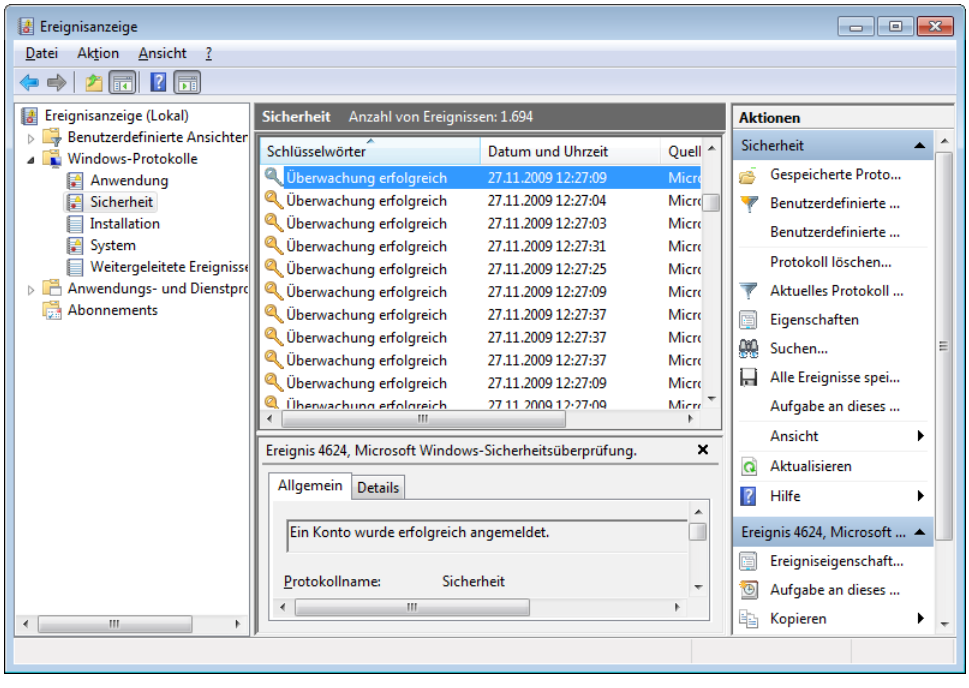


Abbildung 10.26 Überwachen von Anmeldeereignissen

Wenn Sie die Richtlinie *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen\Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen* aktivieren, können Sie die ausführlicheren Überwachungsrichtlinien verwenden, die im Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Systemüberwachungsrichtlinien\Anmelden/Abmelden* verfügbar sind. Dieser Knoten enthält die Richtlinien *Anmelden überwachen* und *Abmelden überwachen*. Diese speziellen Richtlinien verringern die Menge der Aufzeichnungen über Anmelde- und Abmeldeaktivitäten im Ver-

gleich zu der erwähnten allgemeineren Überwachungseinstellung. Die Einträge über An- und Abmeldeversuche aus dem Sicherheitsprotokoll können Sie sich in der Ereignisanzeige ansehen (Abbildung 10.26).



Prüfungstipp

Merken Sie sich, welches Protokoll für VPN-Reconnect erforderlich ist.

Übung Konfigurieren von Remoteverbindungen

Wenn Sie VPN-Verbindungen konfigurieren, müssen Sie drei Dinge wissen: die Adresse des VPN-Servers, den Benutzernamen, mit dem Sie die Verbindung herstellen, und das Kennwort für dieses Konto. Windows 7 probiert alle VPN-Protokolle durch, angefangen mit IKEv2, im nächsten Versuch mit SSTP, dann L2TP/IPsec und schließlich PPTP. Es ist also nicht unbedingt erforderlich, ein Protokoll für die VPN-Verbindung festzulegen. Allerdings können Sie dies später im Eigenschaftendialogfeld einer VPN-Verbindung nachholen. Die folgenden Übungen beschäftigen sich mit der Konfiguration von VPN-Verbindungen.

Übung 1 Konfigurieren einer VPN-Verbindung

In dieser Übung richten Sie eine VPN-Verbindung ein:

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Klicken Sie das Netzwerksymbol mit der rechten Maustaste an und wählen Sie *Netzwerk- und Freigabecenter öffnen*. Es öffnet sich das Netzwerk- und Freigabecenter.
3. Klicken Sie auf *Neue Verbindung oder neues Netzwerk einrichten*. Klicken Sie auf der ersten Seite des Assistenten *Eine Verbindung oder ein Netzwerk einrichten* (Abbildung 10.27) auf *Verbindung mit dem Arbeitsplatz herstellen* und dann auf *Weiter*.

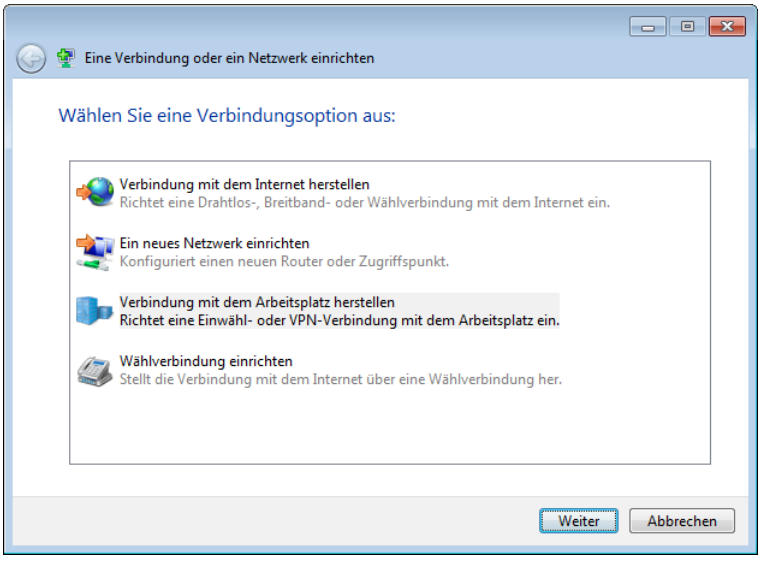

Eine Verbindung oder ein Netzwerk einrichten
Wählen Sie eine Verbindungsoption aus:
Verbindung mit dem Internet herstellen
Richtet eine Drahtlos-, Breitband- oder Wählverbindung mit dem Internet ein.
Ein neues Netzwerk einrichten
Konfiguriert einen neuen Router oder Zugriffspunkt.
Verbindung mit dem Arbeitsplatz herstellen
Richtet eine Einwähl- oder VPN-Verbindung mit dem Arbeitsplatz ein.
Wählverbindung einrichten
Stellt die Verbindung mit dem Internet über eine Wählverbindung her.
Weiter
Abbrechen

Abbildung 10.27 Erstellen einer VPN-Verbindung

4. Klicken Sie auf der Seite *Wie möchten Sie eine Verbindung herstellen?* auf *Die Internetverbindung (VPN) verwenden*.
5. Geben Sie auf der Seite *Geben Sie die Internetadresse zum Herstellen einer Verbindung ein* den Namen **remote-access.contoso.com.** Wählen Sie die Kontrollkästchen *Anderen Benutzern erlauben, diese Verbindung zu verwenden* und *Jetzt nicht verbinden, nur für spätere Verwendung einrichten* (Abbildung 10.28). Klicken Sie auf *Weiter*.

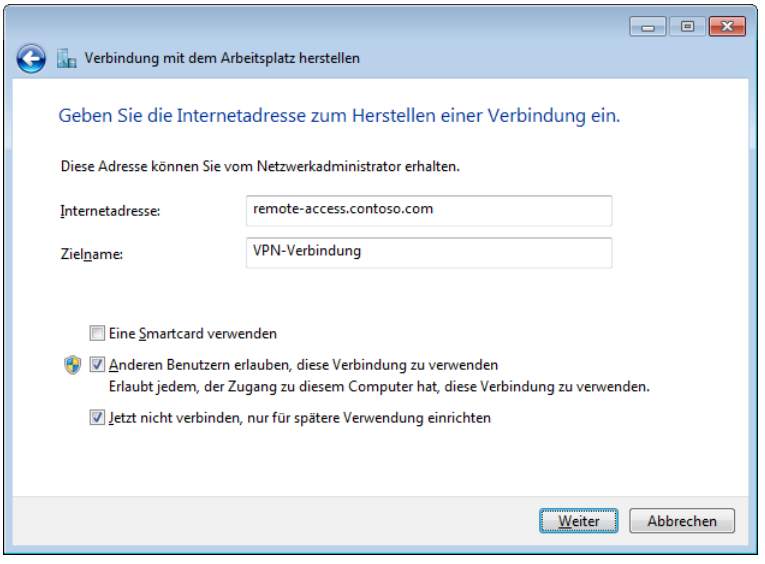

Verbindung mit dem Arbeitsplatz herstellen
Geben Sie die Internetadresse zum Herstellen einer Verbindung ein.
Diese Adresse können Sie vom Netzwerkadministrator erhalten.
Internetadresse:
remote-access.contoso.com
Zielname:
VPN-Verbindung
Eine Smartcard verwenden
Anderen Benutzern erlauben, diese Verbindung zu verwenden
Erlaubt jedem, der Zugang zu diesem Computer hat, diese Verbindung zu verwenden.
Jetzt nicht verbinden, nur für spätere Verwendung einrichten
Weiter
Abbrechen

Abbildung 10.28 VPN-Verbindungsadresse

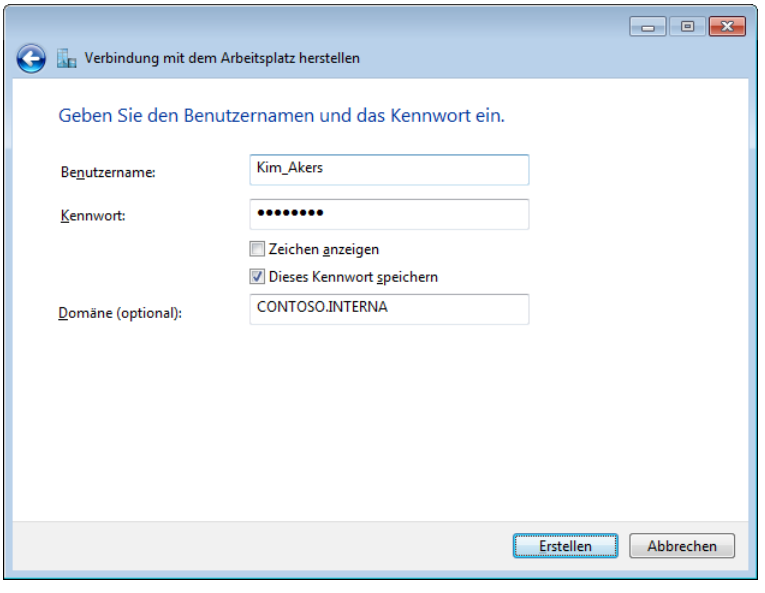


Abbildung 10.29 VPN-Anmeldeinformationen

6. Geben Sie auf der Seite *Geben Sie den Benutzernamen und das Kennwort ein* den Benutzernamen und das Kennwort ein, das zur Authentifizierung beim Routing- und RAS-Server verwendet werden soll. Sie können auch die Domäne des Benutzerkontos eingeben (Abbildung 10.29). Klicken Sie auf *Erstellen* und dann auf *Schließen*.

Übung 2 Ändern der VPN-Verbindungseigenschaften

In dieser Übung ändern Sie die Eigenschaften der VPN-Verbindung, die Sie in der vorigen Übung für den VPN-Server von Contoso konfiguriert haben:

1. Sofern Sie es noch nicht getan haben, melden Sie sich mit dem Benutzerkonto *Kim_Akers* am Computer *Canberra* an.
2. Klicken Sie das Netzwerksymbol mit der rechten Maustaste an und klicken Sie dann auf *Netzwerk- und Freigabecenter öffnen*. Es öffnet sich das Netzwerk- und Freigabecenter.
3. Klicken Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern*.
4. Klicken Sie auf der Seite *Netzwerkverbindungen* des Netzwerk- und Freigabecenters mit der rechten Maustaste auf *VPN-Verbindung* und wählen Sie *Eigenschaften*. Es öffnet sich das Dialogfeld *Eigenschaften von VPN-Verbindung*.
5. Klicken Sie auf die Registerkarte *Sicherheit*. Wählen Sie in der Dropdownliste *VPN-Typ* das Protokoll *IKEv2* (Abbildung 10.30). Durch die Wahl dieses VPN-Typs ändern sich die Authentifizierungsoptionen.

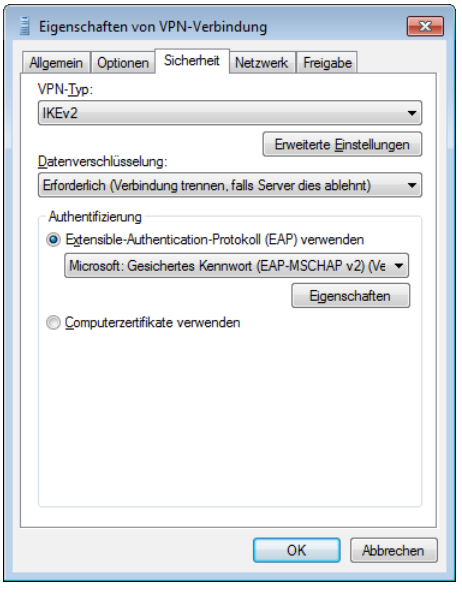


Abbildung 10.30 VPN-Verbindungssicherheit

6. Klicken Sie auf *Erweiterte Einstellungen*. Ändern Sie die *Netzwerkausfallzeit* im Dialogfeld *Erweiterte Eigenschaften* auf 8 Stunden und klicken Sie dann auf *OK*.
7. Schließen Sie das Dialogfeld *Eigenschaften von VPN-Verbindung*.

Zusammenfassung der Lektion

- Windows 7-Clients unterstützen die VPN-Protokolle PPTP, L2TP/IPsec, SSTP und IKEv2.
- Das VPN-Protokoll IKEv2 ist erforderlich, wenn Sie VPN-Reconnect verwenden möchten. Außerdem setzt VPN-Reconnect einen VPN-Server voraus, auf dem Windows Server 2008 R2 ausgeführt wird.
- Das SSTP-Protokoll ermöglicht hinter den meisten Firewalls einen Zugriff auf VPNs, weil es denselben Port wie der HTTPS-Datenverkehr verwendet.
- Remotedesktopgateways erlauben Remotedesktopverbindungen mit Remotedesktophosts aus dem internen Netzwerk einer Organisation, wobei der externe Client keine VPN-Verbindung aufbauen muss. Außerdem ermöglicht Remotedesktopgateway auch die Veröffentlichung von RemoteApp-Anwendungen für Clients aus dem Internet.
- EAP-MS-CHAPv2 ist das sicherste Authentifizierungsprotokoll auf Kennwortbasis und das einzige auf Kennwortbasis, das mit IKEv2 verwendet werden kann.
- Mit dem Assistenten zum Einrichten einer neuen Verbindung, der im Netzwerk- und Freigabecenter zugänglich ist, können Sie eine VPN- oder Wählverbindung einrichten.
- Windows 7 kann als Einwähl- und VPN-Server dienen, wenn Sie eingehende Verbindungen konfigurieren.
- NAP kann verwendet werden, um Remotezugriffe durch Windows 7-Clients zu sperren, die nicht den vorgesehenen Integritätsstandards entsprechen. Diese Clients können in Wartungsnetzwerke umgeleitet werden, in denen die Ressourcen zur Verfügung stehen, um die Clients auf den gewünschten Stand zu bringen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 2, »Remoteverbindungen«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welcher der folgenden VPN-Typen unterstützt VPN-Reconnect?
   A. PPTP
   B. L2TP/IPsec
   C. SSTP
   D. IKEv2
2. Sie arbeiten als Berater für eine kleine Firma, die ein Windows Server 2008-Netzwerk verwendet. Jeder Mitarbeiter dieser Firma verfügt über einen Laptop, auf dem Windows 7 Enterprise verwendet wird. Einige der Mitarbeiter wohnen regelmäßig in verschiedenen kleinen Landmotels. Einige haben sich beschwert, dass sie keine VPN-

Verbindung mit dem Büro herstellen können, obwohl sie über den Internetanschluss des Motels Zugang zum Web haben. Welches der folgenden VPN-Protokolle sollten Sie konfigurieren, um dieses Problem zu beheben?

A. SSTP
B. IKEv2
C. PPTP
D. L2TP/IPsec

3. Auf dem Routing- und RAS-Server Ihrer Organisation wurde Windows Server 2003 R2 installiert. Welches der folgenden Protokolle können Sie verwenden, um eine Verbindung mit dem VPN-Server herzustellen?

   A. SSTP
   B. IKEv2
   C. PPTP
   D. L2TP/IPsec

4. Welche der folgenden Authentifizierungsprotokolle können Sie für eine Verbindung mit einem IKEv2-VPN verwenden? (Wählen Sie alle zutreffenden Antworten.)

   A. PEAP
   B. EAP-MSCHAP v2
   C. Microsoft Smartcard oder anderes Zertifikat
   D. CHAP

5. Sie haben mit Ihrem Computer, auf dem Sie Windows 7 Professional verwenden, eine Verbindung mit einem freien Wi-Fi-Zugriffspunkt hergestellt. Sie möchten eine Verbindung mit dem Server *remote-desktop.contoso.internal* herstellen, um mit einigen speziellen Branchenanwendungen zu arbeiten. Ihre Organisation betreibt unter der Adresse *rdgateway.contoso.com* einen Remotedesktop-Gatewayserver. Derzeit sind auf Ihrem Computer keine VPN-Verbindungen konfiguriert. Wie können Sie eine Verbindung mit *remote-desktop.contoso.internal* herstellen?

   A. Sie konfigurieren eine DirectAccess-Verbindung und stellen dann mit Remotedesktopverbindung eine Verbindung zu *remote-desktop.contoso.internal* her.
   B. Sie konfigurieren die Anwendung Remotedesktopverbindung so, dass sie das Remotedesktopgateway *remote-desktop.contoso.internal* verwendet, und stellen dann eine Verbindung zu *rdgateway.contoso.com* her.
   C. Sie konfigurieren die Anwendung Remotedesktopverbindung so, dass sie das Remotedesktopgateway *rdgateway.contoso.com* verwendet, und stellen dann eine Verbindung zu *remote-desktop.contoso.internal* her.
   D. Sie konfigurieren eine DirectAccess-Verbindung und stellen dann mit Remotedesktopverbindung eine Verbindung zu *rdgateway.contoso.com*.

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- DirectAccess ermöglicht Clients eine Verbindung zu einem internen Netzwerk, sofern eine aktive Internetverbindung verfügbar ist.
- DirectAccess setzt voraus, dass auf den Clients Windows 7 Enterprise oder Ultimate ausgeführt wird und ein DirectAccess-Server zur Verfügung steht, auf dem Windows Server 2008 R2 läuft.
- DirectAccess kann gewöhnliche IPv6-Verbindungen oder IPv6-zu-IPv4-Übergangstechnologien wie Teredo, IP6-zu-IP4 und IP-HTTPS verwenden.
- Windows 7 unterstützt PPTP-, L2TP/IPsec-, SSTP- und IKEv2-VPNs. IKEv2-VPNs unterstützen VPN-Reconnect.
- Remotedesktop-Gatewayserver ermöglichen Remotedesktop Clients, auch ohne eine VPN- oder DirectAccess-Verbindung eine Verbindung mit internen Remotedesktopdiensteservern herzustellen.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **DirectAccess**
- **RemoteApp**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie Ihr Wissen zum Stoff dieses Kapitels an. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: DirectAccess bei Wingtip Toys

Wingtip Toys verfügt derzeit über 40 Laptops, auf denen Windows Vista Business verwendet wird. Wingtip Toys möchte DirectAccess bereitstellen, weil viele Benutzer dieser Computer eine automatische Verbindung mit dem Firmennetzwerk vorziehen, wenn sie sich außer Haus befinden, statt manuell VPN-Verbindungen herstellen zu müssen. Wingtip Toys möchte die vorhandenen Routing- und RAS-Server, die unter Server 2003 R2 x64 betrieben werden, durch einen DirectAccess-Server ersetzen. Dieser Server verfügt über zwei Netzwerkkarten. Seiner Internetschnittstelle wurden zwei aufeinanderfolgende öffentliche IPv4-Adressen zugewiesen. Dieser Server ist Mitglied der Domäne *Wingtiptoys.internal*. Das passende Computerzertifikat wurde bereits auf dem Server installiert.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Welche Schritte sollte Wingtip Toys unternehmen, um den DirectAccess-Server aufzubauen?
2. Welche Gruppe sollten Sie zur Unterstützung von DirectAccess erstellen?
3. Mit welchen Schritten bereiten Sie die Clientcomputer auf die Verwendung von DirectAccess vor?

Übung 2: Remote Access bei Tailspin Toys

Tailspin Toys stellt auf 300 Laptops Windows 7 Professional bereit. Sie möchten sicherstellen, dass zukünftige VPN-Benutzer mit ihren VPN-Sitzungen in Verbindung bleiben können, wenn sie von einer öffentlichen Wi-Fi-Verbindung auf Modemkarten wechseln, die sie von ihrer Firma erhalten. Benutzer sollen sich mit ihren Benutzernamen und Kennwörtern authentifizieren können. Ihre vorhandene VPN-Infrastruktur verwendet NAP. Derzeit wird unter Windows Server 2008 x64 ein Routing- und RAS-Server betrieben. Dieses System sperrt VPN-Zugriffe für Windows Vista-Clients, auf denen nicht die neusten Softwareupdates und Antivirusdefinitionen installiert sind. NAP hält Clients, die nicht den Integritätsanforderungen genügen, vom Zugang zum Netzwerk ab. Diese Clients können keine VPN-Verbindung aufbauen, solange sie nicht direkt ans Firmennetzwerk angeschlossen werden, um Softwareupdates und Antivirusdefinitionen herunterzuladen. Sie möchten nun Ihr Quarantänenetzwerk so aktualisieren, dass nichtkonforme Clients auch über eine Remoteverbindung gewartet werden können. Tailspin Toys verfügt über eine PKI-Infrastruktur, die mit den Active Directory-Zertifikatdiensten aufgebaut wurde.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Was müssen Sie tun, damit das Netzwerk von Tailspin Toys VPN-Reconnect unterstützt?
2. Welche Ergänzungen sollten Sie am Quarantänenetzwerk vornehmen, damit Clients konform werden können?
3. Welches Authentifizierungsprotokoll sollten Sie für Tailspin Toys verwenden?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Konfigurieren von DirectAccess

Führen Sie die folgenden Übungen durch, wenn Sie Zugang zu zwei physischen oder virtuellen Computern haben, auf denen Windows Server 2008 R2 ausgeführt wird:

- **Übung 1** Konfigurieren Sie den ersten Server als Domänencontroller, als DNS-Server und als Active Directory-Zertifikatdiensteserver.
- **Übung 2** Konfigurieren Sie den zweiten Server als DirectAccess-Server. Überprüfen Sie vorher die Voraussetzungen für einen DirectAccess-Server, die in Lektion 1 beschrieben werden.

Konfigurieren von Remoteverbindungen

Führen Sie die folgenden Übungen durch, wenn Sie Zugang zu zwei physischen oder virtuellen Computern haben, auf denen Windows Server 2008 R2 ausgeführt wird:

- **Übung 1** Konfigurieren Sie den ersten Server als Domänencontroller und installieren Sie die Remotedesktopdienste. Konfigurieren Sie den zweiten Server als Remotedesktop-Gatewayserver. Stellen Sie mit einem Windows 7-Client über den Remotedesktop-Gatewayserver eine Verbindung zu den Remotedesktopdiensten auf dem Domänencontroller her.
- **Übung 2** Konfigurieren Sie den ersten Server als Domänencontroller und installieren Sie die Remotedesktopdienste. Konfigurieren Sie den zweiten Server als Routing- und RAS-Server. Stellen Sie mit einem Windows 7-Client, der so konfiguriert ist, dass er nur eine IKEv2-VPN-Verbindung herstellt, eine Verbindung zum Routing- und RAS-Server her.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

KAPITEL 11

BitLocker und Mobilitätsoptionen

Portable Computer bringen für IT-Abteilungen neue Herausforderungen mit sich, die in herkömmlichen Desktopumgebungen nicht auftreten. Eine dieser Herausforderungen besteht darin, für die maximale Betriebsdauer eines portablen Computers zu sorgen, wenn der Computer nicht am Stromnetz angeschlossen ist. Eine weitere ist, dafür zu sorgen, dass der Zugriff auf wichtige Dateien auch dann möglich ist, wenn keine Verbindung mit dem Netzwerk hergestellt werden kann. Als dritte Herausforderung kommt noch hinzu, die Daten so zu schützen, dass ein Unbefugter auch dann nicht Zugriff auf vertrauliche Daten erhält, wenn der portable Computer verloren geht oder gestohlen wird. In diesem Kapitel erfahren Sie etwas von den verschiedenen Technologien, die Ihnen dabei helfen, diese Herausforderungen zu bewältigen.

BitLocker und BitLocker To Go ermöglichen eine Verschlüsselung ganzer Volumes. Dadurch bleiben Daten auch dann geschützt, wenn der Computer oder das Speichergerät, auf dem die Daten liegen, gestohlen wird oder verloren geht. Offlinedateien ermöglichen auch dann den Zugriff auf Daten, die in freigegebenen Netzwerkordnern liegen, wenn ein Computer keine Verbindung mit dem betreffenden Hostcomputer herstellen kann. Die Energieverwaltung von Windows 7 ermöglicht bei Akkubetrieb den optimalen Kompromiss zwischen Systemleistung und Betriebsdauer. Sie können die Leistung erhöhen, wenn die Betriebsdauer nicht so wichtig ist, oder auf möglichst lange Betriebsdauer setzen, wenn Sie den Laptop lange an einem Ort verwenden möchten, wo keine geeignete Stromquelle zur Verfügung steht.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von BitLocker und BitLocker To Go
- Konfigurieren der Mobilitätsoptionen

Lektionen in diesem Kapitel:

- Lektion 1: Verwalten von BitLocker 555
- Lektion 2: Windows 7 und Mobilität 574

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels sind einige Vorbereitungen erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Computer namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.
- Legen Sie ein kleines USB-Speichergerät bereit. Es sollte keine wichtigen Daten enthalten.
- Für die Übung am Ende der Lektion ist kein TPM-Chip (Trusted Platform Module) erforderlich.

Praxistipp

Orin Thomas

Einmal ergab es sich, dass ich ein Kapitel eines Trainingsbuchs nur wenige Minuten vor dem Zeitpunkt zur Bearbeitung zurückerhielt, an dem ich an Bord eines Flugzeugs gehen musste. Das Flugzeug sollte mich von Melbourne, Australien, nach Kopenhagen in Dänemark bringen, mit 2 Stunden Zwischenstopp in Bangkok, Thailand. Das ist eine dieser Reisen, die praktisch um die halbe Welt führen. Da es mir fast nie gelingt, in Flugzeugen zu schlafen, wusste ich also schon beim Abflug, dass ich nach mehr als 24 Stunden Reise nicht würde arbeiten können. Es war besser, das Kapitel jetzt durchzuarbeiten, als mich völlig übernächtigt am anderen Ende der Welt damit herumzuschlagen. Außerdem war ich noch nie in Kopenhagen gewesen und wollte nicht meinen ersten Tag dort damit verbringen, im Hotelzimmer auf der Tastatur meines Computers herumzutippen. Da man für den Preis eines Erste-Klasse-Flugs von Melbourne nach Kopenhagen schon ein kleines Auto kaufen kann, saß ich also in der Touristenklasse, in der es keinen Stromanschluss für meinen Laptop gab. Es kann einige Zeit dauern, ein Kapitel nach der Korrektur durchzuarbeiten. Gewöhnlich dauert es länger, als der Akku meines Laptops durchhält. Es ist keiner dieser neuen Laptops, die im Akkubetrieb angeblich 8 Stunden lang laufen. Immerhin würde er an einem guten Tag etwa 3 Stunden durchhalten, wenn ich ihn nicht zu sehr belastete. Leider brauchte ich für die anstehende Arbeit länger als 3 Stunden. An diesem Punkt bot es sich an, einen speziellen Energiesparplan einzustellen. Ich schaltete praktisch alles aus. Der Bildschirm war sehr dunkel, der Prozessor lief mit wenigen Prozent seiner Höchstgeschwindigkeit, und jedes Gerät, das ich nicht brauchte, war ausgeschaltet. Der Computer reagierte zwar nur schleppend, aber ich konnte auf dem gesamten Flug von Melbourne nach Bangkok mit ihm arbeiten. Zeit genug, um die Arbeit an dem Kapitel abzuschließen. Als ich in Bangkok ankam, reichte der Strom noch aus, um über mein Mobiltelefon eine Verbindung mit dem Internet herzustellen und das überarbeitete Kapitel an meinen Lektor zurückzuschicken. Als ich in Kopenhagen eintraf, konnte ich mich ganz auf eine Stadt konzentrieren, die ich noch nie zuvor gesehen hatte. Eines Tages, wenn ich einen neuen Laptop habe, dessen Akku etwas länger reicht, könnte ich vielleicht einen Energiesparplan einstellen, der für den gesamten Flug von Melbourne nach Kopenhagen reicht. Bis es soweit ist, muss die Strecke von Melbourne nach Bangkok eben reichen!

Lektion 1: Verwalten von BitLocker

Verschiedene Studien haben gezeigt, dass die Belegschaft einer mittelgroßen Firma im Durchschnitt ein bis zwei Laptops im Jahr verliert. Aus diesen Studien geht zudem hervor, dass einer Organisation durch den Verlust eines Laptops Kosten entstehen können, die zwanzigmal höher sind als der eigentliche Wert des Laptops. Es können durchaus einige Zehntausend Dollar werden. Der größte Kostenanteil entsteht durch den Versuch, herauszufinden, welche Daten auf dem Computer gespeichert waren und welche Auswirkungen es hätte, wenn diese Informationen in die Hände der Konkurrenz fielen. Manchmal kann es schwierig werden zu bestimmten, welche Daten auf einem verlorenen Computer gespeichert wurden. Unter ungünstigen Umständen können diese Kosten sehr hoch werden. USB-Flashgeräte (Universal Serial Bus) stellen ein ähnliches Problem dar. Häufig werden sie verwendet, um wichtige Daten zwischen Wohnung und Arbeitsplatz zu transportieren. Da diese Geräte sehr klein sind, gehen sie auch leicht verloren. Wenn eines dieser Geräte verloren geht, besteht eine gewisse geringe Wahrscheinlichkeit dafür, dass sensible Daten ihren Weg in die Hände der Konkurrenz finden.

Bei den Untersuchungen über die Kosten, die durch verlorene Ausrüstung entstehen, hat sich auch ergeben, dass die Kosten, die durch einen verlorenen Laptop entstehen, deutlich geringer sind, wenn die Organisation davon ausgehen kann, dass die Daten auf den Laptops wegen einer vollständigen Verschlüsselung der Laufwerke, wie sie zum Beispiel mit BitLocker möglich ist, geschützt bleiben. In diesen Fällen weiß die betroffene Organisation, dass die Konkurrenz keine wichtigen Daten wiederherstellen kann, die auf einem verlorenen Computer oder Gerät gespeichert sind. Dadurch sinken die Kosten deutlich, weil die Organisation nicht mehr ermitteln muss, welche Daten auf dem verlorenen Gerät gespeichert sein könnten, sondern davon ausgehen kann, dass die Daten praktisch nicht durch andere wiederherzustellen sind. In dieser Lektion erfahren Sie, wie BitLocker und BitLocker To Go unter Windows 7 konfiguriert werden. Wenn Sie dies tun und jemand aus Ihrer Organisation einen Laptop oder ein USB-Flashlaufwerk verliert, können Sie damit rechnen, dass die Person, die das Gerät findet, die auf dem Gerät gespeicherten Daten nicht wiederherstellen kann.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren der Richtlinien für BitLocker und BitLocker To Go
- Verwalten der TPM-PINs
- Konfigurieren des Startschlüsselspeichers
- Konfigurieren der Datenwiederherstellungsagenten

Veranschlagte Zeit für diese Lektion: 40 Minuten

BitLocker

BitLocker ist in den Windows 7-Editionen Enterprise und Ultimate verfügbar und bietet einen Systemschutz durch die vollständige Verschlüsselung aller Volumes. BitLocker hat die Aufgabe, Windows 7-Computer vor Offlineangriffen zu schützen. Zu den Offlineangriffen gehört beispielsweise das Starten eines Computers mit einem anderen Betriebssystem, um Daten von der Festplatte zu kopieren, oder der Versuch, ein Festplattenlaufwerk aus dem Computer auszubauen, an einen anderen Computer anzuschließen und dort zu versuchen, die enthaltenen Daten zu kopieren.

BitLocker ist in der Lage, die Volumes eines Computers vollständig zu verschlüsseln. Ohne den Verschlüsselungsschlüssel sind die auf dem Volume gespeicherten Daten nicht zugänglich. BitLocker speichert den Verschlüsselungsschlüssel für das Volume an einem sicheren Ort und gibt diesen Schlüssel erst frei, macht also die Daten des Volumes erst dann zugänglich, nachdem es die Integrität der Startumgebung überprüft hat.

BitLocker bietet folgende Vorteile:

- Es macht es einem Angreifer unmöglich, Daten von einem gestohlenen Computer wiederherzustellen, sofern er nicht auch die Kennwörter stiehlt, die den Zugang zum Computer ermöglichen. Ohne entsprechende Authentifizierung bleibt das Festplattenlaufwerk verschlüsselt und unzugänglich.
- Es vereinfacht die Entsorgung von Festplattenlaufwerken. Auch ohne die Festplatte eines Computers sorgfältig löschen zu müssen, können Sie davon ausgehen, dass die auf dem Laufwerk gespeicherten Daten ohne den entsprechenden BitLocker-Schlüssel nicht wiederherzustellen sind. Viele Organisationen haben mit Sicherheitsproblemen zu tun gehabt, die sich daraus ergaben, dass Daten von Festplattenlaufwerken wiederhergestellt wurden, nachdem diese Laufwerke ausgemustert worden waren.
- Es schützt die Startumgebung vor unautorisierten Änderungen, indem es sie bei jedem Start des Computers überprüft. Wenn BitLocker in der Startumgebung Änderungen feststellt, zwingt es den Computer in den BitLocker-Wiederherstellungsmodus.

BitLocker bietet zwar gewisse Arten des Schutzes, aber es schützt die auf dem Computer gespeicherten Daten nicht mehr, sobald der Computer vollständig aktiv ist. Wird ein Computer, auf dem BitLocker aktiviert wurde, von mehreren Benutzern verwendet, kann BitLocker die Benutzer nicht daran hindern, die Daten der anderen Benutzer zu lesen, wenn die entsprechenden Datei- und Ordnerberechtigungen nicht korrekt vergeben wurden. BitLocker verschlüsselt zwar das Festplattenlaufwerk, aber diese Verschlüsselung schützt die Daten auf einem hochgefahrenen Computer nicht vor lokalen Angriffen oder vor Angriffen aus dem Netzwerk. Um Daten auf einem laufenden Computer vor unberechtigten Zugriffen zu schützen, können Sie NTFS-Berechtigungen und das verschlüsselnde Dateisystem verwenden. Über diese Technologien haben Sie bereits in Kapitel 8, »BranchCache und Ressourcenfreigabe«, etwas erfahren.



Weitere Informationen Überblick über BitLocker für Führungskräfte

Eine ausführlichere Beschreibung der BitLocker-Funktionen unter Windows 7 finden Sie in folgendem Übersichtsdokument im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/dd548341(WS.10).aspx.*

BitLocker-Modi

BitLocker kann in verschiedenen Modi verwendet werden. Welcher Modus sinnvoll ist, hängt davon ab, ob auf Ihrem Computer ein TPM (Trusted Platform Module) zur Verfügung steht und welchen Grad an Sicherheit Sie erreichen wollen. Die Modi ergeben sich daraus, welche Kombination von TPM, PIN (Personal Identification Number) und Startschlüssel gewählt wird. Ein Startschlüssel ist eine spezielle, mit kryptografischen Methoden generierte Datei, die auf einem separaten USB-Laufwerk gespeichert wird. Folgende BitLocker-Modi sind verfügbar:

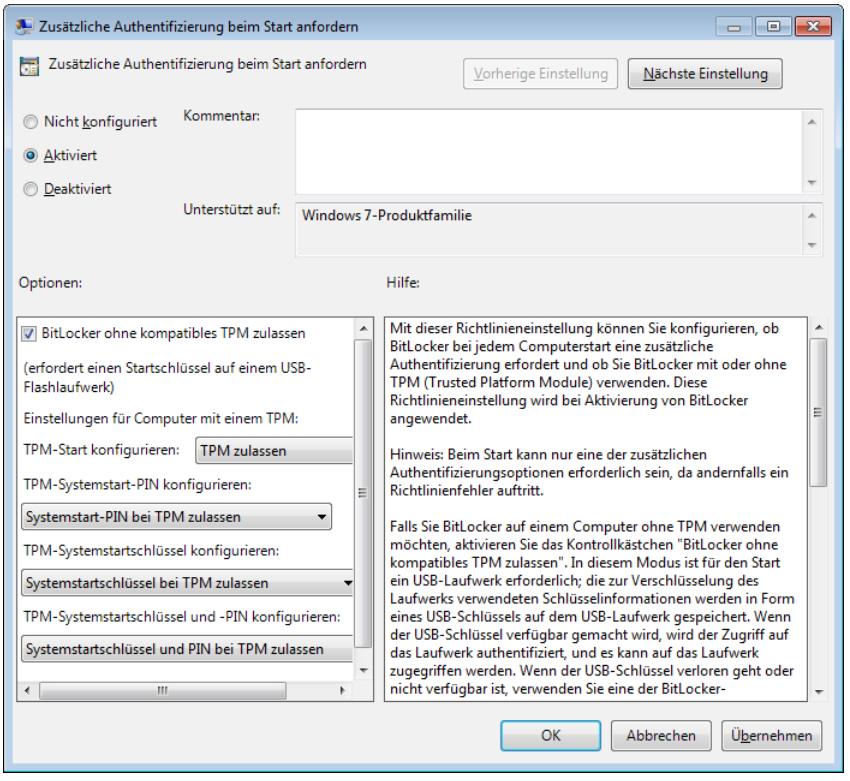

Zusätzliche Authentifizierung beim Start anfordern
Zusätzliche Authentifizierung beim Start anfordern
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Windows 7-Produktfamilie
Optionen:
Hilfe:
BitLocker ohne kompatibles TPM zulassen
(erfordert einen Startschlüssel auf einem USB-Flashlaufwerk)
Einstellungen für Computer mit einem TPM:
TPM-Start konfigurieren:
TPM zulassen
TPM-Systemstart-PIN konfigurieren:
Systemstart-PIN bei TPM zulassen
TPM-Systemstartschlüssel konfigurieren:
Systemstartschlüssel bei TPM zulassen
TPM-Systemstartschlüssel und -PIN konfigurieren:
Systemstartschlüssel und PIN bei TPM zulassen
Mit dieser Richtlinieneinstellung können Sie konfigurieren, ob BitLocker bei jedem Computerstart eine zusätzliche Authentifizierung erfordert und ob Sie BitLocker mit oder ohne TPM (Trusted Platform Module) verwenden. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.
Hinweis: Beim Start kann nur eine der zusätzlichen Authentifizierungsoptionen erforderlich sein, da andernfalls ein Richtlinienfehler auftritt.
Falls Sie BitLocker auf einem Computer ohne TPM verwenden möchten, aktivieren Sie das Kontrollkästchen "BitLocker ohne kompatibles TPM zulassen". In diesem Modus ist für den Start ein USB-Laufwerk erforderlich; die zur Verschlüsselung des Laufwerks verwendeten Schlüsselinformationen werden in Form eines USB-Schlüssels auf dem USB-Laufwerk gespeichert. Wenn der USB-Schlüssel verfügbar gemacht wird, wird der Zugriff auf das Laufwerk authentifiziert, und es kann auf das Laufwerk zugegriffen werden. Wenn der USB-Schlüssel verloren geht oder nicht verfügbar ist, verwenden Sie eine der BitLocker-
OK
Abbrechen
Übernehmen

Abbildung 11.1 Zulassen der Verwendung von BitLocker ohne TPM-Chip

- **Nur TPM** In diesem Modus ist sich der Benutzer nicht notwendigerweise bewusst, dass sein Computer durch BitLocker geschützt wird. Er braucht keine Kennwörter, keine PINs und keine Startschlüssel anzugeben, um seinen Computer zu starten. Der Benutzer wird erst dann auf BitLocker aufmerksam, wenn eine Änderung der Startumgebung erfolgt oder wenn er die Festplatte in einen anderen Computer einbaut und dort verwenden möchte. Dieser Modus ist der unsicherste BitLocker-Modus, weil keine zusätzliche Authentifizierung erforderlich ist.
- **TPM mit Startschlüssel** Dieser Modus erfordert, das beim Start des Computers ein USB-Laufwerk mit einem vorkonfigurierten Startschlüssel verfügbar ist, damit Windows 7 starten kann. Ist zur Startzeit kein USB-Gerät mit einem Startschlüssel verfügbar, wechselt der Computer in den Wiederherstellungsmodus. Der Modus bietet durch das TPM einen Schutz der Startumgebung.
- **TPM mit PIN** Wenn Sie diesen Modus konfigurieren, muss der Benutzer eine PIN eingeben, damit sich der Computer starten lässt. In den Gruppenrichtlinien können Sie zudem festlegen, dass statt einer PIN ein regelrechtes Kennwort mit Ziffern, Buchstaben und Sonderzeichen eingegeben werden muss. Wird beim Start des Computers nicht die korrekte PIN oder das korrekte Kennwort eingegeben, wechselt der Computer in den Wiederherstellungsmodus. Der Modus bietet durch das TPM einen Schutz der Startumgebung.

- **TPM mit Startschlüssel und PIN** Das ist der sicherste Modus. Sie können ihn in den Gruppenrichtlinien einstellen. Wenn Sie diesen Modus wählen, muss ein Benutzer eine PIN eingeben und das Gerät, auf dem der Startschlüssel gespeichert ist, mit dem Computer verbinden, damit sich der Computer mit Windows starten lässt. Der Modus eignet sich zum Beispiel für Hochsicherheitsumgebungen. Durch das TPM bietet er einen Schutz der Startumgebung.
- **BitLocker ohne TPM** Dieser Modus bietet zwar eine Verschlüsselung des Festplattenlaufwerks, aber keinen Schutz der Startumgebung. Er wird auf Computern verwendet, die nicht über ein TPM verfügen. Damit sich BitLocker auf solchen Computern verwenden lässt, müssen Sie die Richtlinie *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Betriebssystemlaufwerke\Zusätzliche Authentifizierung beim Start anfordern* konfigurieren (Abbildung 11.1). Wenn Sie BitLocker für den Betrieb ohne TPM-Chip konfigurieren, müssen Sie für den Start auf einem USB-Laufwerk einen Startschlüssel bereitstellen.

Verwalten des TPM-Chips

Die meisten Implementierungen von BitLocker speichern den Verschlüsselungsschlüssel auf einem speziellen Chip der Computerhardware, der TPM-Chip (Trusted Platform Module) genannt wird. Die TPM-Verwaltungskonsole (Abbildung 11.2) ermöglicht Administratoren die Verwaltung des TPM. Mit dieser Konsole können Sie TPM-Wiederherstellungsinformationen in den Active Directory-Domänendiensten (Active Directory Domain Services, AD DS) speichern, das TPM löschen, eine TPM-Sperrung aufheben und das TPM aktivieren oder deaktivieren. Sie erreichen die TPM-Verwaltungskonsole, indem Sie auf der Seite *BitLocker-Laufwerkverschlüsselung* der Systemsteuerung auf das Element *TPM-Verwaltung* klicken.

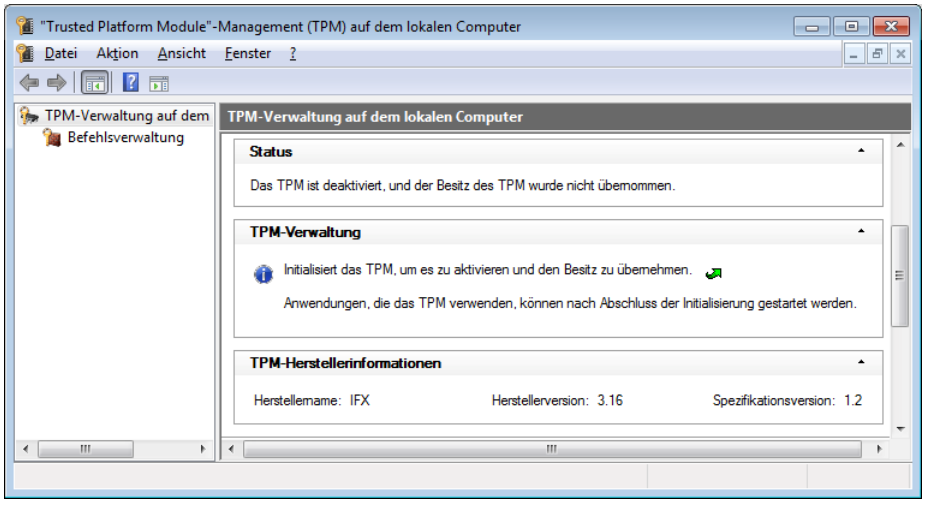

"Trusted Platform Module"-Management (TPM) auf dem lokalen Computer
Datei Aktion Ansicht Fenster ?
TPM-Verwaltung auf dem
Befehlsverwaltung
TPM-Verwaltung auf dem lokalen Computer
Status
Das TPM ist deaktiviert, und der Besitz des TPM wurde nicht übernommen.
TPM-Verwaltung
Initialisiert das TPM, um es zu aktivieren und den Besitz zu übernehmen.
Anwendungen, die das TPM verwenden, können nach Abschluss der Initialisierung gestartet werden.
TPM-Herstellerinformationen
Herstellername: IFX
Herstellerversion: 3.16
Spezifikationsversion: 1.2

Abbildung 11.2 TPM-Verwaltungskonsole

Konfigurieren eines Datenwiederherstellungsagenten für BitLocker

Datenwiederherstellungsagenten (Data Recovery Agents, DRAs) sind spezielle Benutzerkonten für die Wiederherstellung von verschlüsselten Daten. Sie können einen DRA einrichten, um Daten von BitLocker-geschützten Laufwerken wiederherzustellen, falls das Wiederherstellungskennwort oder der Schlüssel verloren geht. Der Vorteil eines DRAs ist seine organisationsweite Verwendbarkeit, d.h. sämtliche BitLocker-verschlüsselten Volumes lassen sich mit einem einzigen Konto wiederherstellen, nicht nur ein bestimmtes Volume.

Der erste Schritt bei der Einrichtung eines Wiederherstellungsagenten für BitLocker besteht darin, das Konto des DRAs zum Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel\BitLocker-Laufwerkverschlüsselung* hinzuzufügen (Abbildung 11.3). Ein DRA-Konto ist ein Benutzerkonto, für das eine bestimmte Art von digitalem Zertifikat ausgestellt wurde. In einer Organisationsumgebung wird dieses digitale Zertifikat praktisch immer von einer Zertifizierungsstelle ausgestellt.

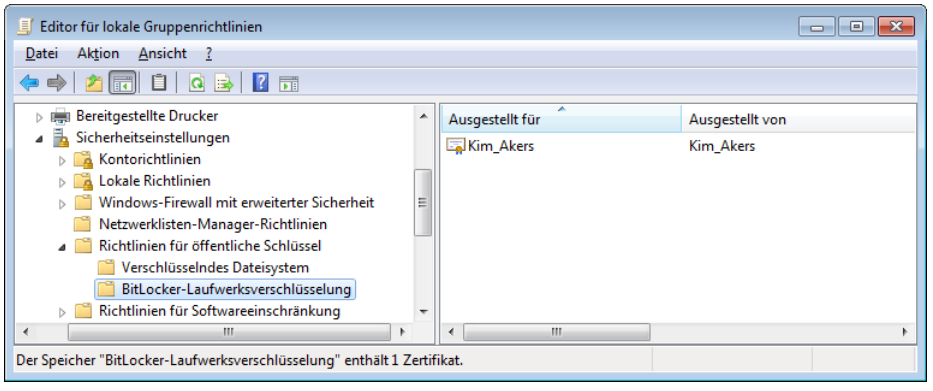


Abbildung 11.3 Zuweisen eines Datenwiederherstellungsagenten

Nachdem Sie den DRA konfiguriert haben, müssen Sie auch die Richtlinie *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Eindeutige IDs für Ihre Organisation angeben* konfigurieren, damit die Wiederherstellung durch einen DRA möglich wird. BitLocker akzeptiert DRAs nur, wenn auf einem Volume ein Identifikationsfeld vorhanden ist und der Wert mit dem Wert übereinstimmt, der für den Computer konfiguriert wurde. Abbildung 11.4 zeigt diese Richtlinie mit dem Wert *ContosoBitLockerSelfHost* im ID-Feld. Diese Richtlinie wird auch verwendet, wenn Schreibzugriffe auf Wechselgeräte gesperrt werden sollen, die nicht durch BitLocker geschützt sind. Über die Sperrung von Schreibzugriffen auf solche Wechselgeräte erfahren Sie mehr im Verlauf der Lektion.

Nachdem Sie den DRA und die Kennungen konfiguriert haben, müssen Sie noch folgende Richtlinien konfigurieren, damit bestimmte Volumetypen den DRA verwenden können:

- *Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können*
- *Festlegen, wie BitLocker-geschützte Festplattenlaufwerke wiederhergestellt werden können*
- *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können*

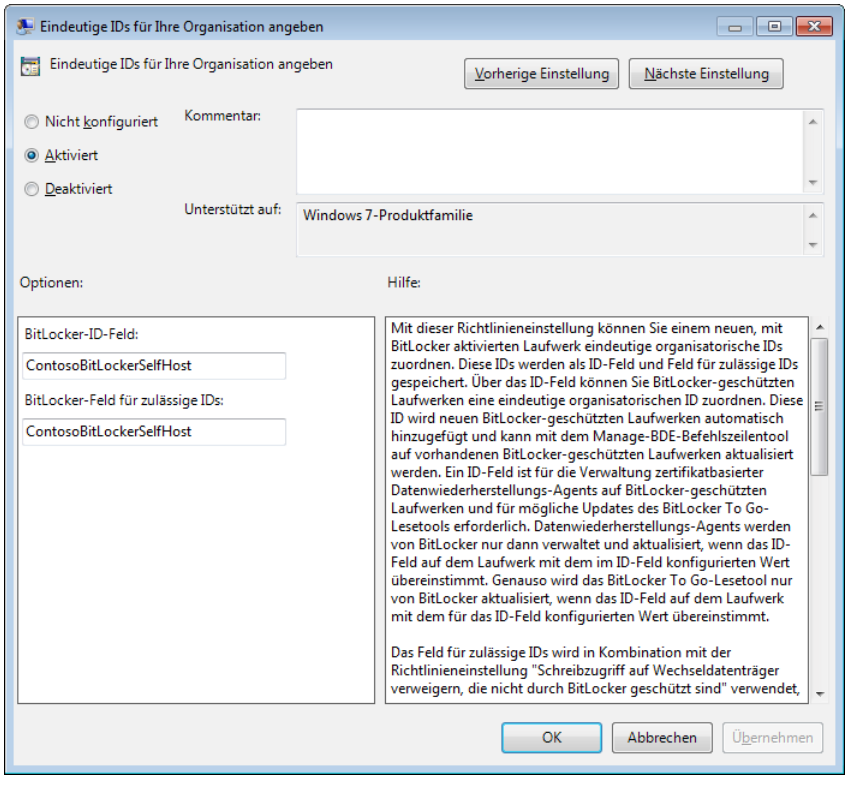

Eindeutige IDs für Ihre Organisation angeben
Eindeutige IDs für Ihre Organisation angeben
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Windows 7-Produktfamilie
Optionen:
Hilfe:
BitLocker-ID-Feld:
ContosoBitLockerSelfHost
BitLocker-Feld für zulässige IDs:
ContosoBitLockerSelfHost
Mit dieser Richtlinieneinstellung können Sie einem neuen, mit BitLocker aktivierten Laufwerk eindeutige organisatorische IDs zuordnen. Diese IDs werden als ID-Feld und Feld für zulässige IDs gespeichert. Über das ID-Feld können Sie BitLocker-geschützten Laufwerken eine eindeutige organisatorischen ID zuordnen. Diese ID wird neuen BitLocker-geschützten Laufwerken automatisch hinzugefügt und kann mit dem Manage-BDE-Befehlszeilentool auf vorhandenen BitLocker-geschützten Laufwerken aktualisiert werden. Ein ID-Feld ist für die Verwaltung zertifikatbasierter Datenwiederherstellungs-Agents auf BitLocker-geschützten Laufwerken und für mögliche Updates des BitLocker To Go-Lesetools erforderlich. Datenwiederherstellungs-Agents werden von BitLocker nur dann verwaltet und aktualisiert, wenn das ID-Feld auf dem Laufwerk mit dem im ID-Feld konfigurierten Wert übereinstimmt. Genauso wird das BitLocker To Go-Lesetool nur von BitLocker aktualisiert, wenn das ID-Feld auf dem Laufwerk mit dem für das ID-Feld konfigurierten Wert übereinstimmt.
Das Feld für zulässige IDs wird in Kombination mit der Richtlinieneinstellung "Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind" verwendet,
OK
Abbrechen
Übernehmen

Abbildung 11.4 Konfigurieren eindeutiger Kennungen

Jede dieser Richtlinien lässt sich so einstellen, dass der DRA zugelassen wird. Sie können auch für jeden Volumetyp ein Wiederherstellungskennwort und einen Wiederherstellungsschlüssel konfigurieren (Abbildung 11.5). Sie können jedes der Elemente, die Sie in diesen Richtlinien angeben, zur Wiederherstellung verwenden. In den Richtlinien können Sie auch dafür sorgen, dass die Wiederherstellungskennwörter und -schlüssel in AD DS gespeichert werden. Es ist sogar möglich, die Einrichtung von BitLocker so lange zu sperren, bis diese Daten erfolgreich in AD DS gespeichert sind. Sie sollten die Sicherung der Wiederherstellungsinformationen in AD DS nicht aktivieren, wenn die Windows 7-Clients keine Domänenmitglieder sind.

Es kann sich die Situation ergeben, dass BitLocker bereits auf einem Volume aktiviert wurde, bevor Sie einen DRA einrichten. Mit dem Befehl `manage-bde -SetIdentifier` können Sie in einer Eingabeaufforderung mit erhöhten Rechten dafür sorgen, dass das Volume einen DRA unterstützt. Verwenden Sie dann den Befehl `manage-bde -status` und überprüfen Sie in der Ausgabe den Wert im *ID-Feld*. Wenn Sie überprüfen möchten, ob der DRA korrekt konfiguriert wurde, verwenden Sie den Befehl `manage-bde -protectors -get`. Dadurch wird der Fingerabdruck des DRA-Zertifikats aufgelistet. Zur Wiederherstellung von Daten von einem Volume, für das ein DRA konfiguriert wurde, verbinden Sie das Volume mit einem funktionierenden Computer, auf dem der private DRA-Schlüssel installiert ist, und verwenden in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `Manage-bde.exe -unlock <Laufwerk> -Certificate -ct <Zertifikatfingerabdruck>`. Einige dieser Befehle verwenden Sie in der Übung am Ende dieser Lektion.

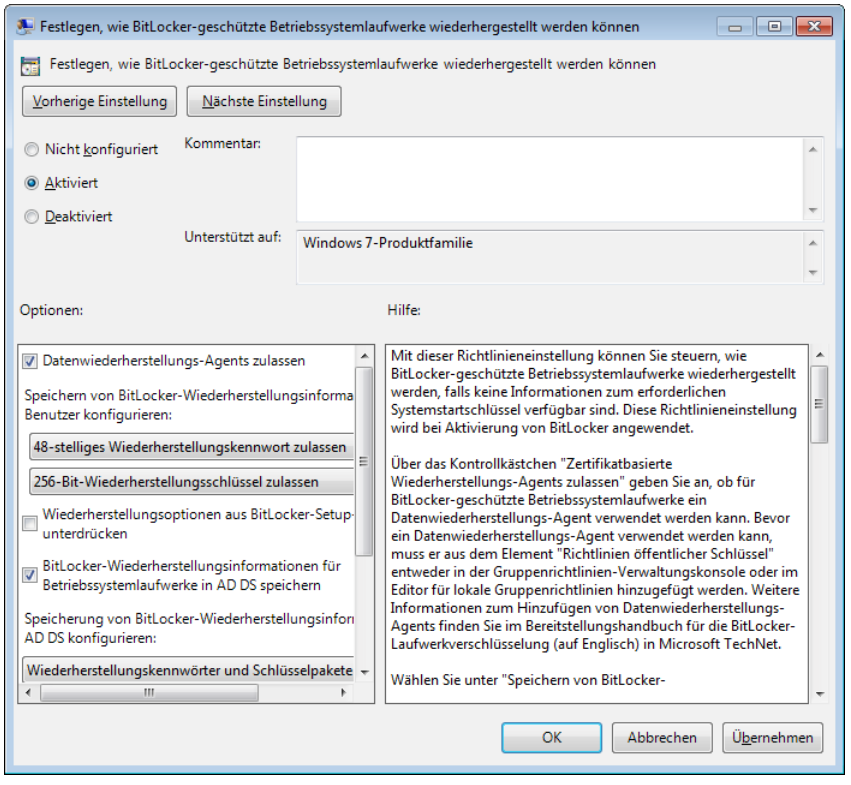

Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können
Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Windows 7-Produktfamilie
Optionen:
Hilfe:
Datenwiederherstellungs-Agents zulassen
Speichern von BitLocker-Wiederherstellungsinforma
Benutzer konfigurieren:
48-stelliges Wiederherstellungskennwort zulassen
256-Bit-Wiederherstellungsschlüssel zulassen
Wiederherstellungsoptionen aus BitLocker-Setup
unterdrücken
BitLocker-Wiederherstellungsinformationen für
Betriebssystemlaufwerke in AD DS speichern
Speicherung von BitLocker-Wiederherstellungsinfor
AD DS konfigurieren:
Wiederherstellungskennwörter und Schlüsselpakete
Mit dieser Richtlinieneinstellung können Sie steuern, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden, falls keine Informationen zum erforderlichen Systemstartschlüssel verfügbar sind. Diese Richtlinieneinstellung wird bei Aktivierung von BitLocker angewendet.
Über das Kontrollkästchen "Zertifikatbasierte Wiederherstellungs-Agents zulassen" geben Sie an, ob für BitLocker-geschützte Betriebssystemlaufwerke ein Datenwiederherstellungs-Agent verwendet werden kann. Bevor ein Datenwiederherstellungs-Agent verwendet werden kann, muss er aus dem Element "Richtlinien öffentlicher Schlüssel" entweder in der Gruppenrichtlinien-Verwaltungskonsole oder im Editor für lokale Gruppenrichtlinien hinzugefügt werden. Weitere Informationen zum Hinzufügen von Datenwiederherstellungs-Agents finden Sie im Bereitstellungshandbuch für die BitLocker-Laufwerkverschlüsselung (auf Englisch) in Microsoft TechNet.
Wählen Sie unter "Speichern von BitLocker-
OK
Abbrechen
Übernehmen

Abbildung 11.5 Wiederherstellungsrichtlinien



Weitere Informationen **Konfigurieren eines Datenwiederherstellungsagenten für BitLocker**

Weitere Informationen über das Konfigurieren eines Datenwiederherstellungsagenten für BitLocker finden Sie in dem folgenden Microsoft TechNet-Artikel: *http://technet.microsoft.com/en-us/library/dd875560(WS.10).aspx.*

Aktivieren von BitLocker

Um BitLocker auf einem Computer zu aktivieren, öffnen Sie in der Systemsteuerung die Seite *BitLocker-Laufwerkverschlüsselung* und klicken dann auf *BitLocker aktivieren*. Ein Benutzer muss Mitglied der lokalen Gruppe *Administratoren* sein, um auf einem Windows 7-Computer BitLocker aktivieren zu können. Wenn Sie auf *BitLocker aktivieren* klicken, wird überprüft, ob die entsprechende TPM-Hardware vorhanden ist oder ob die Gruppenrichtlinien so konfiguriert sind, dass BitLocker auch ohne TPM zugelassen wird. Ist keine TPM-Hardware vorhanden und sind die Gruppenrichtlinien nicht entsprechend konfiguriert, werden Sie mit einer Fehlermeldung darüber informiert, dass kein TPM gefunden wurde und der Systemadministrator BitLocker aktivieren muss.

Der nächste Schritt ist die Wahl des Authentifizierungsmodus für BitLocker. Die verschiedenen BitLocker-Modi haben Sie in dieser Lektion bereits kennengelernt: Nur TPM, TPM mit Startschlüssel, TPM mit PIN sowie TPM mit Startschlüssel und PIN. Wenn Sie BitLocker ohne TPM verwenden, können Sie nur einen Startschlüssel verlangen (Abbildung 11.6). Der Modus TPM mit Startschlüssel und PIN lässt sich nur in den Gruppenrichtlinien festlegen.

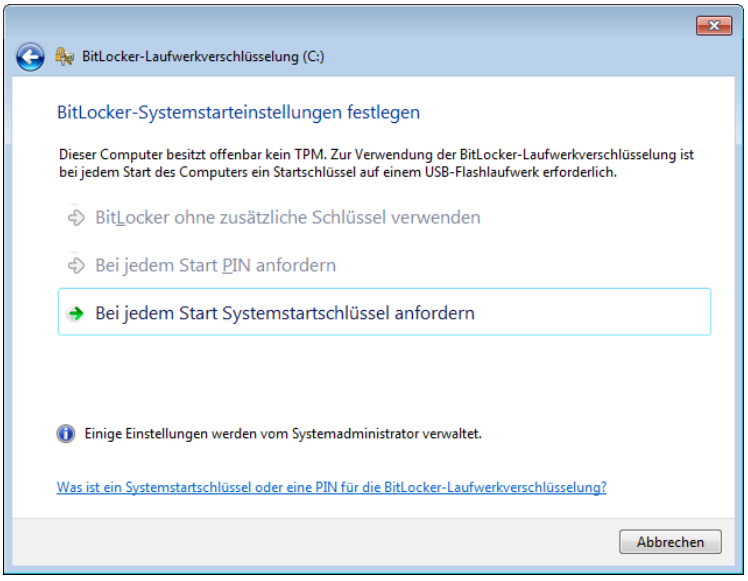

BitLocker-Laufwerkverschlüsselung (C:)
BitLocker-Systemstarteinstellungen festlegen
Dieser Computer besitzt offenbar kein TPM. Zur Verwendung der BitLocker-Laufwerkverschlüsselung ist bei jedem Start des Computers ein Startschlüssel auf einem USB-Flashlaufwerk erforderlich.
BitLocker ohne zusätzliche Schlüssel verwenden
Bei jedem Start PIN anfordern
Bei jedem Start Systemstartschlüssel anfordern
Einige Einstellungen werden vom Systemadministrator verwaltet.
Was ist ein Systemstartschlüssel oder eine PIN für die BitLocker-Laufwerkverschlüsselung?
Abbrechen

Abbildung 11.6 Konfigurieren der Startoptionen für BitLocker

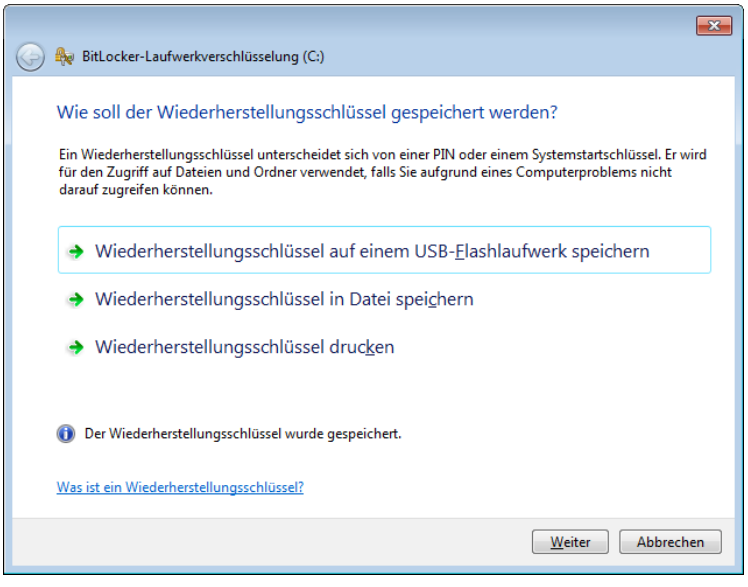

BitLocker-Laufwerkverschlüsselung (C:)
Wie soll der Wiederherstellungsschlüssel gespeichert werden?
Ein Wiederherstellungsschlüssel unterscheidet sich von einer PIN oder einem Systemstartschlüssel. Er wird für den Zugriff auf Dateien und Ordner verwendet, falls Sie aufgrund eines Computerproblems nicht darauf zugreifen können.
Wiederherstellungsschlüssel auf einem USB-Flashlaufwerk speichern
Wiederherstellungsschlüssel in Datei speichern
Wiederherstellungsschlüssel drucken
Der Wiederherstellungsschlüssel wurde gespeichert.
Was ist ein Wiederherstellungsschlüssel?
Weiter
Abbrechen

Abbildung 11.7 Speichern des Wiederherstellungsschlüssels

Wenn bei jedem Start ein Startschlüssel angegeben werden soll, fordert Windows Sie auf, ein USB-Speichergerät auszuwählen, auf dem der Schlüssel gespeichert werden soll. Dann schreibt Windows den Schlüssel auf das ausgewählte Gerät. Im nächsten Schritt wird der Wiederherstellungsschlüssel gespeichert (Abbildung 11.7). Der Wiederherstellungsschlüssel unterscheidet sich vom Startschlüssel und der PIN. Sie sollten den Wiederherstellungsschlüssel an einem anderen Ort speichern als den Startschlüssel. Falls Sie dann den Startschlüssel verlieren, haben Sie nicht auch noch den Wiederherstellungsschlüssel verloren.

Der letzte Schritt vor der Aktivierung von BitLocker auf einem Computer ist eine Systemüberprüfung (Abbildung 11.8). Dabei wird überprüft, ob BitLocker das Laufwerk verschlüsseln kann und ob es Probleme mit dem Startschlüssel oder dem TPM-Chip gibt. Diese Überprüfung dauert zwar einige Zeit, aber Sie sollten diesen Schritt nicht überspringen, denn alle auf dem Computer befindlichen Daten könnten verloren gehen, falls er sich nicht für BitLocker eignet. Wenn Sie zum Beispiel BitLocker ohne TPM verwenden, finden Sie durch diese Überprüfung heraus, ob das USB-Gerät, auf dem Sie den Startschlüssel gespeichert haben, vor dem Start von Windows für den Computer zugänglich ist. Auch wenn der Startschlüssel auf diesem Gerät vorhanden ist, unterstützt das BIOS vielleicht den Zugriff auf das USB-Gerät nicht zum erforderlichen Zeitpunkt und BitLocker sperrt den Computer. Sollte das der Fall sein, können Sie BitLocker nicht auf diesem Computer verwenden. Es ist wesentlich besser, ein solches Problem vor der Aktivierung von BitLocker zu erkennen, als die Wiederherstellungsprozedur von BitLocker zu verwenden.

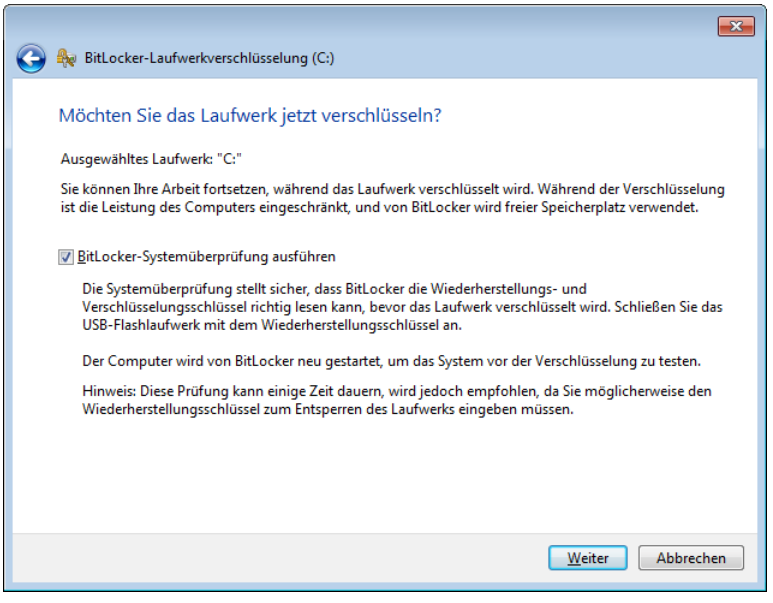

BitLocker-Laufwerkverschlüsselung (C:)
Möchten Sie das Laufwerk jetzt verschlüsseln?
Ausgewähltes Laufwerk: "C:"
Sie können Ihre Arbeit fortsetzen, während das Laufwerk verschlüsselt wird. Während der Verschlüsselung ist die Leistung des Computers eingeschränkt, und von BitLocker wird freier Speicherplatz verwendet.
BitLocker-Systemüberprüfung ausführen
Die Systemüberprüfung stellt sicher, dass BitLocker die Wiederherstellungs- und Verschlüsselungsschlüssel richtig lesen kann, bevor das Laufwerk verschlüsselt wird. Schließen Sie das USB-Flashlaufwerk mit dem Wiederherstellungsschlüssel an.
Der Computer wird von BitLocker neu gestartet, um das System vor der Verschlüsselung zu testen.
Hinweis: Diese Prüfung kann einige Zeit dauern, wird jedoch empfohlen, da Sie möglicherweise den Wiederherstellungsschlüssel zum Entsperren des Laufwerks eingeben müssen.
Weiter
Abbrechen

Abbildung 11.8 Durchführen einer Systemüberprüfung vor der Verwendung von BitLocker

Zum Systemtest gehört auch ein Neustart des Computers. Nach erfolgreichem Test beginnt BitLocker mit der Verschlüsselung. Die Verschlüsselung wird im Hintergrund durchgeführt. Ein Benutzer mit Administratorrechten kann die Verschlüsselung bei Bedarf anhalten und wieder weiterlaufen lassen. BitLocker ist erst dann aktiv und wirksam, wenn die Verschlüsselung abgeschlossen ist.

Schnelltest

- Welche Richtlinie müssen Sie konfigurieren, damit ein Computer ohne TPM-Chip BitLocker verwenden kann, wobei der Startschlüssel auf einem kompatiblen USB-Gerät gespeichert wird?

Antwort zum Schnelltest

- Sie müssen die Richtlinie *Zusätzliche Authentifizierung beim Start anfordern* konfigurieren, damit ein Computer, der nicht über einen TPM-Chip verfügt, BitLocker verwenden kann und der Startschlüssel auf einem kompatiblen USB-Gerät gespeichert werden kann.

BitLocker To Go

BitLocker To Go ist in den Editionen Enterprise und Ultimate von Windows 7 verfügbar. Mit Computern, auf denen diese Windows 7-Editionen verwendet werden, können USB-Laufwerke für BitLocker To Go konfiguriert werden. Andere Editionen von Windows 7 können zwar Daten von BitLocker To Go-Geräten lesen und schreiben, aber sie können USB-Geräte nicht für BitLocker To Go konfigurieren. BitLocker To Go ermöglicht die Verschlüsselung von Wechseldatenträgern mit BitLocker. BitLocker To Go unterscheidet sich insofern von den BitLocker-Versionen älterer Windows-Versionen, als ein mit BitLocker verschlüsselter Wechseldatenträger an andere Computer angeschlossen und dort verwendet werden kann, wenn man über das entsprechende Kennwort verfügt. Unter Windows Vista SP1 und höher war es zwar möglich, Wechseldatenträger mit BitLocker zu verschlüsseln, aber diese Geräte dann an anderen Computern zu verwenden war nicht einfach und erforderte die Durchführung einer BitLocker-Wiederherstellung.

BitLocker To Go setzt keinen TPM-Chip voraus und auch nicht, dass die Gruppenrichtlinien eine andere Authentifizierung als den Startschlüssel zulassen. Wenn Sie die entsprechenden Richtlinien konfigurieren, können mit BitLocker To Go geschützte Geräte unter Windows XP und Windows Vista zumindest gelesen werden.

Richtlinien für BitLocker To Go

Der Knoten *Wechseldatenträger* der Richtlinie BitLocker-Laufwerkverschlüsselung enthält 6 Richtlinien für die Verwaltung von BitLocker To Go (Abbildung 11.9).

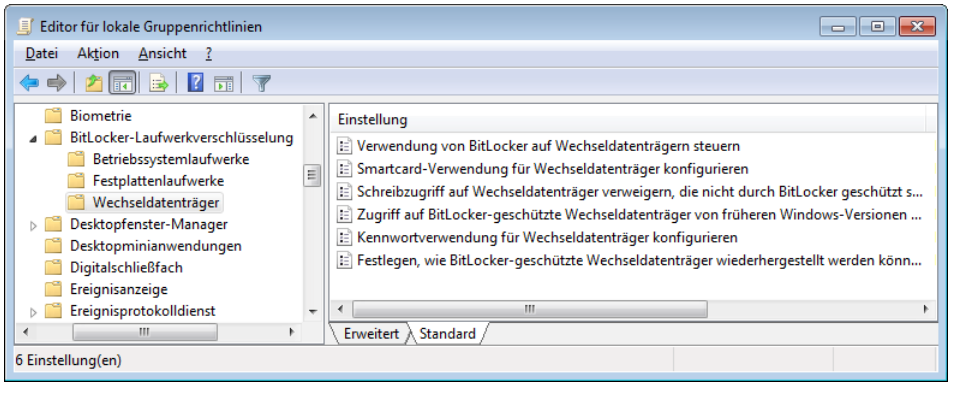


Abbildung 11.9 Richtlinien für Wechseldatenträger

- **Verwendung von BitLocker auf Wechseldatenträgern steuern** Diese Richtlinie enthält 2 Einstellungen, die sich aktivieren lassen. Die erste erlaubt Benutzern die Anwendung von BitLocker auf Wechsellaufwerken. Die zweite erlaubt Benutzern, den

BitLocker-Schutz auf Wechsellaufwerken anzuhalten und das Laufwerk zu entschlüsseln. Wenn diese Richtlinie deaktiviert ist, lässt sich BitLocker To Go nicht verwenden.

- **Smartcard-Verwendung für Wechseldatenträger konfigurieren** Mit dieser Richtlinie können Sie die Verwendung von Smartcards zur Authentifizierung von Zugriffen auf Wechsellaufwerke zulassen oder verbindlich festlegen. Ist die Richtlinie deaktiviert, können Benutzer für die Authentifizierung bei Zugriffen auf BitLocker-geschützte Wechsellaufwerke keine Smartcards verwenden.
- **Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind** Mit dieser Richtlinie werden Benutzer daran gehindert, auf Wechselgeräte zu schreiben, die nicht BitLocker-geschützt sind. In der Richtlinie können Sie das Kontrollkästchen *Keinen Schreibzugriff auf Geräte zulassen, die in anderen Organisationen konfiguriert wurden* aktivieren, um Schreibzugriffe auf Wechselgeräte zu beschränken, die über eine bestimmte BitLocker-Kennung verfügen. Diese Kennung wird mit der bereits beschriebenen Richtlinie *Eindeutige IDs für Ihre Organisation angeben* festgelegt (siehe auch Abbildung 11.4). Wenn diese Richtlinie aktiviert ist, können Benutzer immer noch Daten von Wechselgeräten lesen, die nicht mit BitLocker geschützt sind oder nicht über die gewünschte Kennung verfügen. Wenn die Richtlinie deaktiviert ist, können Benutzer unabhängig davon, ob ein Wechselgerät mit BitLocker geschützt ist, Daten auf das Gerät schreiben.
- **Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen** Mit dieser Richtlinie können Sie festlegen, ob BitLocker-geschützte und mit dem FAT-Dateisystem formatierte Wechselgeräte unter älteren Windows-Versionen zugänglich sein sollen. Die Richtlinie gilt nicht für Wechselgeräte, die mit NTFS-formatiert sind. Sie können diese Richtlinie verwenden, um die Installation des BitLocker To Go-Lesetools zuzulassen. Das ist ein Programm, mit dem auf älteren Windows-Versionen Daten gelesen werden können, die auf BitLocker-geschützten Wechselgeräten gespeichert wurden. Das BitLocker To Go-Lesetool muss auf diesen älteren Computern verfügbar sein, wenn Daten von Wechselgeräten gelesen werden sollen, die mit BitLocker geschützt sind. Wenn diese Richtlinie deaktiviert ist, lassen sich mit FAT formatierte, BitLocker-geschützte Wechselgeräte auf Computern, auf denen ältere Windows-Versionen verwendet werden, nicht entsperren.
- **Kennwortverwendung für Wechseldatenträger konfigurieren** Diese Richtlinie legt fest, ob ein Kennwort erforderlich ist, um ein mit BitLocker geschütztes Wechsellaufwerk zu entsperren (Abbildung 11.10). Mit der Richtlinie lassen sich auch Mindestanforderungen an die Komplexität der Kennwörter festlegen. Wenn die Richtlinie deaktiviert ist, können Benutzer für Wechselgeräte keine Kennwörter verwenden.
- **Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können** Mit dieser Richtlinie legen Sie fest, wie BitLocker-geschützte Wechselgeräte wiederhergestellt werden können. Sie können den DRA für Wechsellaufwerke zulassen, der im Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel\BitLocker-Laufwerkverschlüsselung* angegeben wurde. Sie können auch ein Wiederherstellungskennwort und einen Wiederherstellungsschlüssel festlegen. Außerdem können Sie festlegen, ob die Wiederherstellungsinformationen in AD DS gespeichert werden.

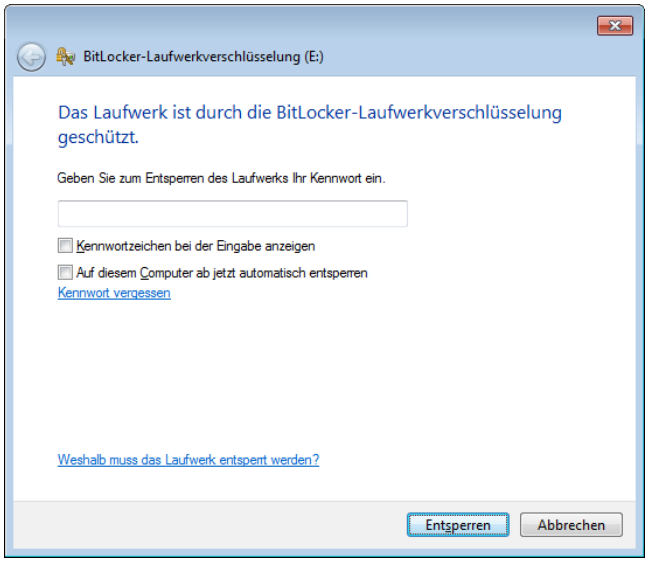

BitLocker-Laufwerkverschlüsselung (E:)
Das Laufwerk ist durch die BitLocker-Laufwerkverschlüsselung geschützt.
Geben Sie zum Entsperren des Laufwerks Ihr Kennwort ein.
Kennwortzeichen bei der Eingabe anzeigen
Auf diesem Computer ab jetzt automatisch entsperren
Kennwort vergessen
Weshalb muss das Laufwerk entsperrt werden?
Entsperren
Abbrechen

Abbildung 11.10 Kennwörter für den Zugriff auf verschlüsselte Wechseldatenträgern

Zur Verwaltung eines Wechseldatenträgers, der BitLocker To Go unterstützt, kann man es im Windows-Explorer mit der rechten Maustaste anklicken oder auf der Seite *BitLocker-Laufwerkverschlüsselung* der Systemsteuerung auf das entsprechende Element *BitLocker verwalten* klicken. Dadurch öffnet sich das in Abbildung 11.11 gezeigte Dialogfeld. Es ermöglicht die Änderung des Kennworts für das Laufwerk, die Umstellung des Laufwerks auf eine Entsperrung mit Smartcard, die erneute Speicherung des Wiederherstellungsschlüssels, die Entfernung des Kennworts oder die automatische Entsperrung nach dem Anschließen des Geräts an einen Computer.

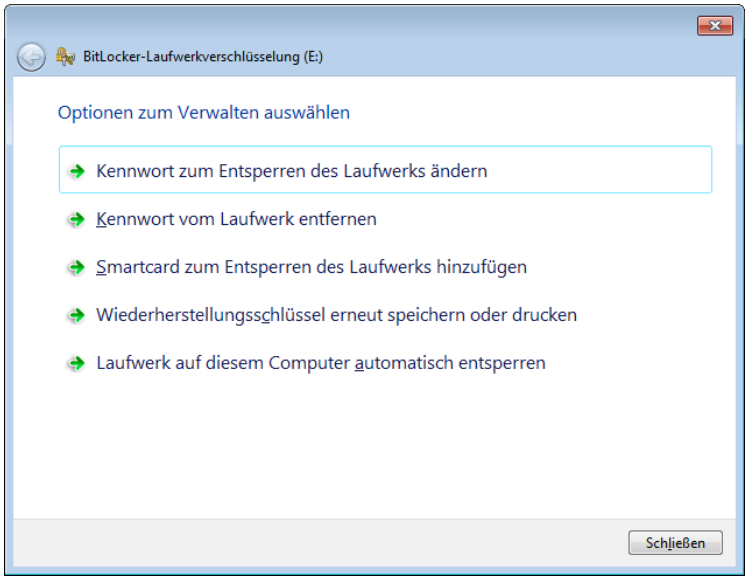

BitLocker-Laufwerkverschlüsselung (E:)
Optionen zum Verwalten auswählen
Kennwort zum Entsperren des Laufwerks ändern
Kennwort vom Laufwerk entfernen
Smartcard zum Entsperren des Laufwerks hinzufügen
Wiederherstellungsschlüssel erneut speichern oder drucken
Laufwerk auf diesem Computer automatisch entsperren
Schließen

Abbildung 11.11 Verwaltungsoptionen für BitLocker To Go

BitLocker-Wiederherstellung

Verschlüsselte Volumes werden gesperrt, wenn der Verschlüsselungsschlüssel nicht verfügbar ist. Wenn das Betriebssystemvolume gesperrt ist, können Sie den Computer nur in den Wiederherstellungsmodus starten. Im Wiederherstellungsmodus können Sie das BitLocker-Kennwort eingeben oder ein USB-Gerät anschließen, auf dem der Wiederherstellungsschlüssel gespeichert ist, und den Computer neu starten. Nach der Eingabe des Wiederherstellungsschlüssels oder -kennworts können Sie den Computer normal starten. Folgende Ereignisse lösen einen Wechsel in den Wiederherstellungsmodus aus:

- Es wurden Änderungen der Startumgebung vorgenommen. Das könnte zum Beispiel bedeuten, dass eine der Startdateien geändert wurde.
- Das TPM wurde deaktiviert oder gelöscht.
- Es wurde der Versuch unternommen, den Computer ohne TPM, PIN oder USB-Schlüssel zu starten.
- Das mit BitLocker verschlüsselte Betriebssystemvolume wurde an einen anderen Computer angeschlossen.

Wenn Sie eine Aufgabe durchführen, die normalerweise einen Wechsel in den Wiederherstellungsmodus auslöst, beispielsweise eine Änderung der Startdateien, können Sie BitLocker temporär deaktivieren. Sie sollten BitLocker temporär deaktivieren, wenn Sie das BIOS des Computers aktualisieren oder Änderungen in der Startumgebung durchführen und zum Beispiel Windows 7 für einen Dual-Boot mit einer VHD-Installation (Virtual Hard Disk) des Betriebssystems konfigurieren. Nach erfolgter Konfigurationsänderung können Sie BitLocker wieder aktivieren. Die Änderungen, die Sie durchgeführt haben, während BitLocker deaktiviert war, lösen keinen Wechsel in den Wiederherstellungsmodus aus.

Manage-bde.exe

Manage-bde.exe ist ein Befehlszeilenprogramm zur Verwaltung von BitLocker. Es wird in einer Eingabeaufforderung mit erhöhten Rechten verwendet. *Manage-bde.exe* ermöglicht die Entsperrung von gesperrten BitLocker-Volumes und die Änderung von BitLocker-PINs, -Kennwörtern und -Schlüsseln. Tabelle 11.1 listet die gebräuchlichsten Parameter von *Manage-bde.exe* auf. In einer Übung am Ende der Lektion verwenden Sie *Manage-bde.exe*.

Tabelle 11.1 Gebräuchliche Parameter für *Manage-bde.exe*

Parameter	Beschreibung
`-status`	Zeigt den BitLocker-Status an.
`-on`	Verschlüsselt ein Volume und schaltet BitLocker ein
`-off`	Entschlüsselt ein Volume und schaltet BitLocker aus
`-pause/-resume`	Hält die Ver- oder Entschlüsselung an oder lässt sie weiterlaufen
`-lock`	Verhindert den Zugriff auf durch BitLocker verschlüsselte Daten
`-unlock`	Lässt den Zugriff auf durch BitLocker verschlüsselte Daten zu
`-SetIdentifier`	Konfiguriert das ID-Feld für ein Volume
`-changepin`	Ändert die PIN für ein Volume
`-changepassword`	Ändert das Kennwort für ein Volume
`-changekey`	Ändert den Startschlüssel für ein Volume



Prüfungstipp

Merken Sie sich, welche Richtlinie Sie konfigurieren müssen, damit BitLocker auf Computern ohne TPM-Chip verwendet werden kann.

Übung Konfigurieren von BitLocker To Go

In dieser Übung konfigurieren Sie die Gruppenrichtlinien so, dass Benutzer Daten nur auf speziell vorbereitete Wechseldatenträger schreiben können, die BitLocker To Go unterstützen. In der Praxis würde diese Maßnahme dafür sorgen, dass Daten, die auf einem Wechseldatenträger gespeichert wurden, vor Zugriffen anderer geschützt sind, falls das Speichergerät irgendwo verloren geht.

Übung 1 Konfigurieren der Richtlinien für BitLocker To Go

In dieser Übung nehmen Sie Gruppenrichtlinieneinstellungen für BitLocker To Go vor.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Sorgen Sie dafür, dass das USB-Speichergerät, das Sie mit BitLocker To Go verschlüsseln möchten, am Computer angeschlossen ist.
3. Verwenden Sie die Konsole *Datenträgerverwaltung*, um das USB-Speichergerät mit dem Dateisystem FAT32 zu formatieren.

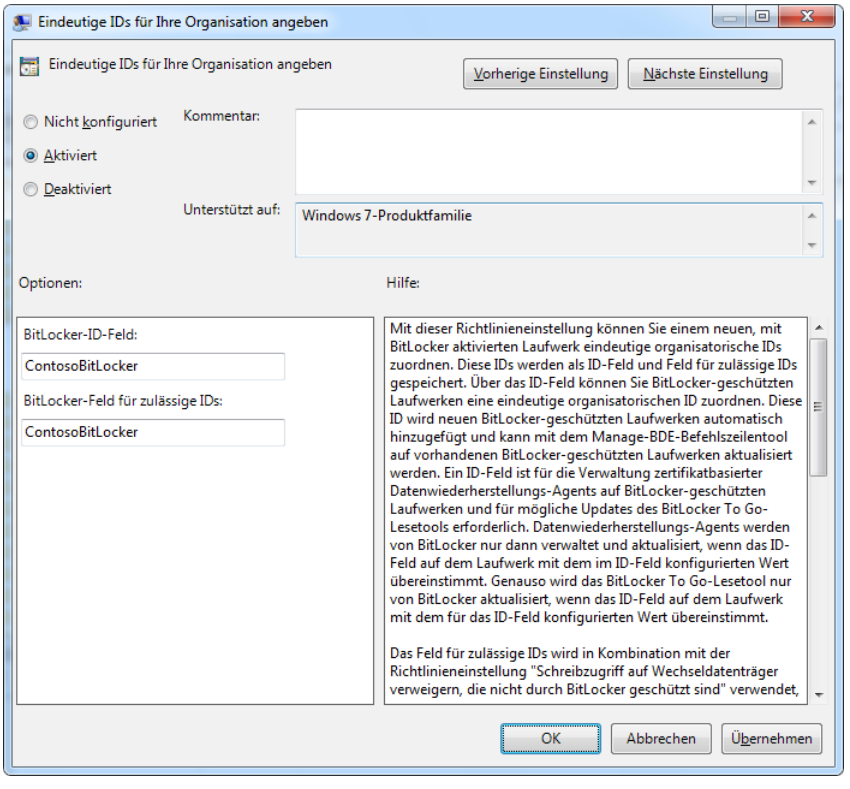

Eindeutige IDs für Ihre Organisation angeben
Eindeutige IDs für Ihre Organisation angeben
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Windows 7-Produktfamilie
Optionen:
Hilfe:
BitLocker-ID-Feld:
ContosoBitLocker
BitLocker-Feld für zulässige IDs:
ContosoBitLocker
Mit dieser Richtlinieneinstellung können Sie einem neuen, mit BitLocker aktivierten Laufwerk eindeutige organisatorische IDs zuordnen. Diese IDs werden als ID-Feld und Feld für zulässige IDs gespeichert. Über das ID-Feld können Sie BitLocker-geschützten Laufwerken eine eindeutige organisatorischen ID zuordnen. Diese ID wird neuen BitLocker-geschützten Laufwerken automatisch hinzugefügt und kann mit dem Manage-BDE-Befehlszeilentool auf vorhandenen BitLocker-geschützten Laufwerken aktualisiert werden. Ein ID-Feld ist für die Verwaltung zertifikatbasierter Datenwiederherstellungs-Agents auf BitLocker-geschützten Laufwerken und für mögliche Updates des BitLocker To Go-Lesetools erforderlich. Datenwiederherstellungs-Agents werden von BitLocker nur dann verwaltet und aktualisiert, wenn das ID-Feld auf dem Laufwerk mit dem im ID-Feld konfigurierten Wert übereinstimmt. Genauso wird das BitLocker To Go-Lesetool nur von BitLocker aktualisiert, wenn das ID-Feld auf dem Laufwerk mit dem für das ID-Feld konfigurierten Wert übereinstimmt.
Das Feld für zulässige IDs wird in Kombination mit der Richtlinieneinstellung "Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind" verwendet,
OK
Abbrechen
Übernehmen

Abbildung 11.12 Konfigurieren der Kennungen

4. Trennen Sie das USB-Speichergerät von Computer.
5. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Gpedit.msc** ein. Dadurch öffnet sich der Editor für lokale Gruppenrichtlinien.
6. Navigieren Sie zu dem Knoten *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung*.
7. Bearbeiten Sie die Richtlinie *Eindeutige IDs für Ihre Organisation angeben*. Aktivieren Sie die Richtlinie und tragen Sie in den Textfeldern *BitLocker-ID-Feld* und *BitLocker-Feld für zulässige IDs* die Kennung **ContosoBitLocker** ein (Abbildung 11.12). Klicken Sie dann auf *OK*.
8. Öffnen Sie den Knoten *Wechseldatenträger* und aktivieren Sie die Richtlinie *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind*. Wählen Sie dann das Kontrollkästchen *Keinen Schreibzugriff auf Geräte zulassen, die in anderen Organisationen konfiguriert wurden*. Klicken Sie auf *OK*.
9. Aktivieren Sie die Richtlinie *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen*.
10. Aktivieren Sie die Richtlinie *Kennwortverwendung für Wechseldatenträger konfigurieren*. Wählen Sie das Kontrollkästchen *Kennwort für Wechseldatenträger anfordern* und in der Dropdownliste *Kennwortkomplexität für Wechseldatenträger konfigurieren* den Eintrag *Kennwortkomplexität zulassen* (Abbildung 11.13). Klicken Sie auf *OK*.

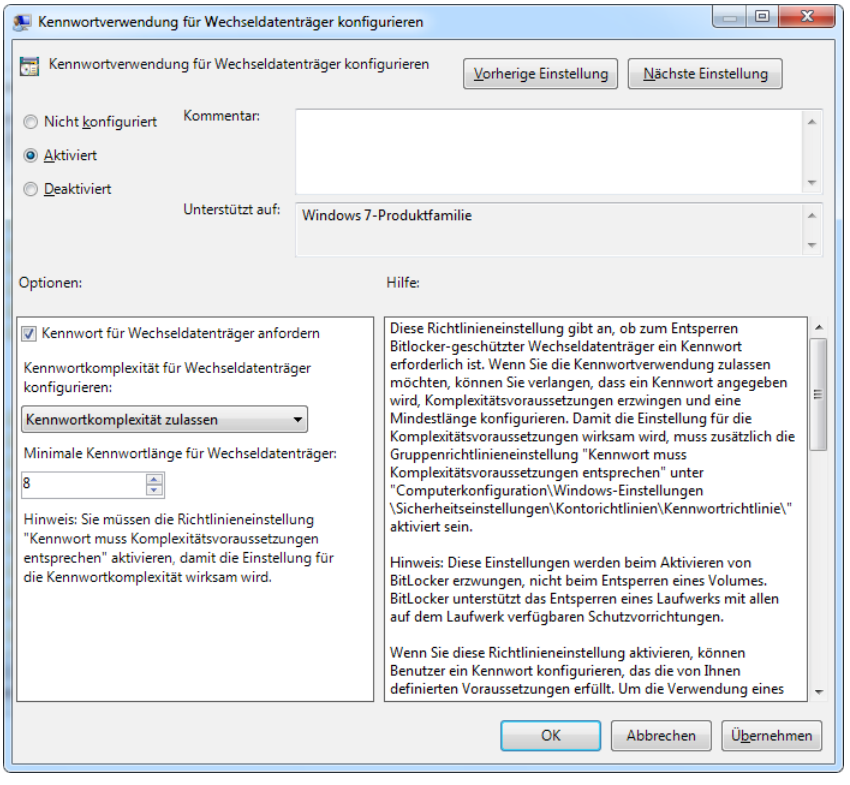

Kennwortverwendung für Wechseldatenträger konfigurieren
Kennwortverwendung für Wechseldatenträger konfigurieren
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Windows 7-Produktfamilie
Optionen:
Hilfe:
Kennwort für Wechseldatenträger anfordern
Kennwortkomplexität für Wechseldatenträger konfigurieren:
Kennwortkomplexität zulassen
Minimale Kennwortlänge für Wechseldatenträger:
8
Hinweis: Sie müssen die Richtlinieneinstellung "Kennwort muss Komplexitätsvoraussetzungen entsprechen" aktivieren, damit die Einstellung für die Kennwortkomplexität wirksam wird.
Diese Richtlinieneinstellung gibt an, ob zum Entsperren Bitlocker-geschützter Wechseldatenträger ein Kennwort erforderlich ist. Wenn Sie die Kennwortverwendung zulassen möchten, können Sie verlangen, dass ein Kennwort angegeben wird, Komplexitätsvoraussetzungen erzwingen und eine Mindestlänge konfigurieren. Damit die Einstellung für die Komplexitätsvoraussetzungen wirksam wird, muss zusätzlich die Gruppenrichtlinieneinstellung "Kennwort muss Komplexitätsvoraussetzungen entsprechen" unter "Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Kontorichtlinien\Kennwortrichtlinie\" aktiviert sein.
Hinweis: Diese Einstellungen werden beim Aktivieren von BitLocker erzwungen, nicht beim Entsperren eines Volumes. BitLocker unterstützt das Entsperren eines Laufwerks mit allen auf dem Laufwerk verfügbaren Schutzvorrichtungen.
Wenn Sie diese Richtlinieneinstellung aktivieren, können Benutzer ein Kennwort konfigurieren, das die von Ihnen definierten Voraussetzungen erfüllt. Um die Verwendung eines
OK
Abbrechen
Übernehmen

Abbildung 11.13 Konfigurieren der Kennwortkomplexität für Wechseldatenträger

11. Schließen Sie den Editor für lokale Gruppenrichtlinien und starten Sie den Computer neu.

Übung 2 Anwenden der Richtlinien für BitLocker To Go

In dieser Übung verschlüsseln Sie ein auswechselbares Speichergerät und überprüfen, ob sich Daten nur auf Geräte schreiben lassen, die mit BitLocker verschlüsselt werden.

1. Melden Sie sich nach dem Neustart des Computers *Canberra* am Ende von Übung 1 mit dem Benutzerkonto *Kim_Akers* an.
2. Schließen Sie das USB-Speichergerät an, das Sie in Übung 1 vorbereitet haben. Überprüfen Sie, ob die in Abbildung 11.14 gezeigte Meldung erscheint.

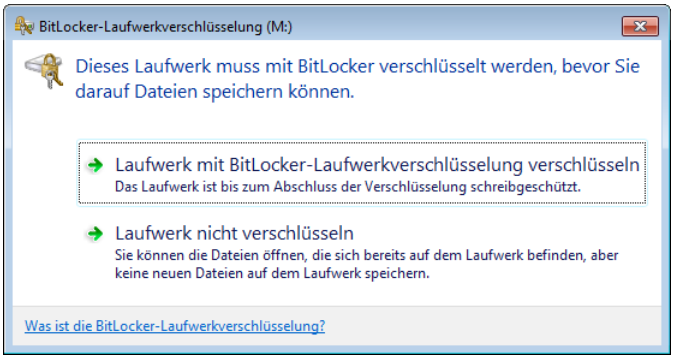

BitLocker-Laufwerkverschlüsselung (M:)
Dieses Laufwerk muss mit BitLocker verschlüsselt werden, bevor Sie darauf Dateien speichern können.
Laufwerk mit BitLocker-Laufwerkverschlüsselung verschlüsseln
Das Laufwerk ist bis zum Abschluss der Verschlüsselung schreibgeschützt.
Laufwerk nicht verschlüsseln
Sie können die Dateien öffnen, die sich bereits auf dem Laufwerk befinden, aber keine neuen Dateien auf dem Laufwerk speichern.
Was ist die BitLocker-Laufwerkverschlüsselung?

Abbildung 11.14 Wechselbare Speichergeräte müssen verschlüsselt werden

3. Klicken Sie auf *Laufwerk nicht verschlüsseln*, um das Dialogfeld zu schließen. Erstellen Sie auf dem Desktop eine Datei namens *Test.txt*. Versuchen Sie, diese Datei mit dem Windows-Explorer auf das USB-Speichergerät zu kopieren. Dabei erhalten Sie eine Meldung mit dem Hinweis, dass der Datenträger schreibgeschützt ist.
4. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **BitLocker verwalten** ein**.** Klicken Sie auf das Element *BitLocker verwalten*.
5. Klicken Sie auf der Seite *BitLocker-Laufwerkverschlüsselung* der Systemsteuerung neben dem USB-Wechsellaufwerk auf *BitLocker aktivieren* (Abbildung 11.15).
6. Geben Sie auf der Seite *Methode zum Entsperren des Laufwerks auswählen* zweimal das Kennwort **P@ssw0rd** ein und klicken Sie dann auf *Weiter*. (Heben Sie dazu bei Bedarf kurzfristig den Schreibschutz des Laufwerks in den Gruppenrichtlinien auf.)
7. Klicken Sie auf der Seite *Wie soll der Wiederherstellungsschlüssel gespeichert werden?* auf *Wiederherstellungsschlüssel in Datei speichern* und speichern Sie den Wiederherstellungsschlüssel dann auf dem Desktop. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Möchten Sie das Laufwerk jetzt verschlüsseln?* auf *Verschlüsselung starten*. Windows beginnt mit der Verschlüsselung des Laufwerks.
9. Wenn die Verschlüsselung des Laufwerks abgeschlossen ist, öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und verwenden den Befehl **manage-bde -status e:** (darin ist *e:* die Laufwerksnummer des USB-Speichergeräts). Überprüfen Sie, ob die Einstellung des ID-Felds *ContosoBitLocker* lautet (Abbildung 11.16).

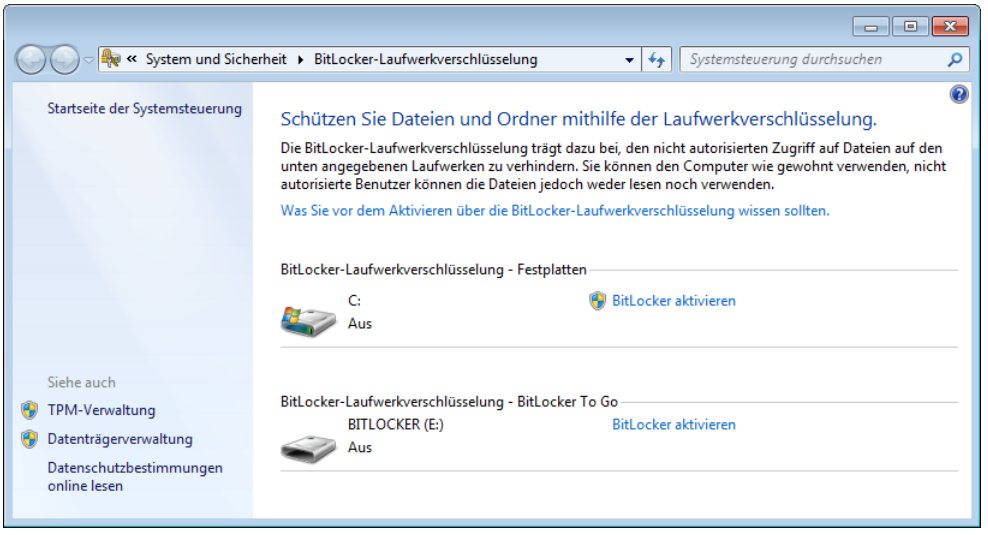

« System und Sicherheit ▸ BitLocker-Laufwerkverschlüsselung
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Schützen Sie Dateien und Ordner mithilfe der Laufwerkverschlüsselung.
Die BitLocker-Laufwerkverschlüsselung trägt dazu bei, den nicht autorisierten Zugriff auf Dateien auf den unten angegebenen Laufwerken zu verhindern. Sie können den Computer wie gewohnt verwenden, nicht autorisierte Benutzer können die Dateien jedoch weder lesen noch verwenden.
Was Sie vor dem Aktivieren über die BitLocker-Laufwerkverschlüsselung wissen sollten.
BitLocker-Laufwerkverschlüsselung - Festplatten
C:
Aus
BitLocker aktivieren
BitLocker-Laufwerkverschlüsselung - BitLocker To Go
BITLOCKER (E:)
Aus
BitLocker aktivieren
Siehe auch
TPM-Verwaltung
Datenträgerverwaltung
Datenschutzbestimmungen online lesen

Abbildung 11.15 Die BitLocker-Steuerung



Abbildung 11.16 Überprüfen des BitLocker-Status

10. Versuchen Sie erneut, die Datei *Test.txt* mit dem Windows-Explorer vom Desktop auf das USB-Speichergerät zu kopieren. Überprüfen Sie, ob sich die Daten nun auf das Laufwerk schreiben lassen.
11. Trennen Sie das Laufwerk und schließen Sie es wieder an. Überprüfen Sie, ob Sie nun ein Kennwort eingeben müssen, damit Sie auf das Laufwerk zugreifen können.

Zusammenfassung der Lektion

- BitLocker bietet eine vollständige Laufwerkverschlüsselung für Computer, auf denen die Windows 7-Editionen Enterprise oder Ultimate ausgeführt werden.
- Damit BitLocker die Integrität der Startumgebung überprüfen und schützen kann, sind TPM-Chips erforderlich. TPM-PINs können in AD DS gespeichert werden.
- BitLocker kann in fünf verschiedenen Modi betrieben werden: Nur TPM, TPM mit PIN, TPM mit Startschlüssel, TPM mit Startschlüssel und PIN sowie Startschlüssel ohne TPM. Der Modus Startschlüssel ohne TPM lässt sich mit der Gruppenrichtlinie *Zusätzliche Authentifizierung beim Start anfordern* aktivieren.
- Zur Wiederherstellung von Volumes, die mit BitLocker verschlüsselt wurden, können Datenwiederherstellungsagenten (Data Recovery Agents, DRAs) konfiguriert werden.
- BitLocker To Go bietet eine BitLocker-Verschlüsselung für auswechselbare Speichergeräte. Solche Geräte können auf Computern konfiguriert werden, auf denen die Editionen Enterprise oder Ultimate von Windows 7 verwendet wird. Mit anderen Editionen von Windows 7 können solche Wechselgeräte zwar nicht konfiguriert werden, aber es sind Lese- und Schreibzugriffe auf mit BitLocker To Go geschützte Wechseldatenträger möglich.
- Auswechselbare Speichergeräte, die mit BitLocker To Go geschützt werden, können zusätzlich durch Kennwörter geschützt werden.
- Unter Windows Vista und Windows XP sind mit einem Hilfsprogramm namens BitLocker To Go-Lesetool Zugriffe auf Speichergeräte möglich, die mit BitLocker To Go geschützt werden, sofern die Gruppenrichtlinien dies zulassen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Verwalten von BitLocker«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welche der folgenden Richtlinien müssen Sie konfigurieren, um einen Datenwiederherstellungsagenten einzurichten, der ein mit BitLocker verschlüsseltes Betriebssystemvolume wiederherstellen kann? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)
   A. *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Eindeutige IDs für Ihre Organisation angeben*
   B. *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Standardordner für Wiederherstellungskennwort auswählen*

C. *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Wiederherstellungsoptionen für BitLocker-geschützte Laufwerke für Benutzer auswählen*

D. *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel\BitLocker-Laufwerkverschlüsselung*

E. *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Betriebssystemlaufwerke\Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können*

2. Sie möchten Benutzer daran hindern, Daten auf Wechsellaufwerken zu speichern, wenn diese Laufwerke nicht durch BitLocker geschützt werden. Benutzer sollen auch keine Daten auf BitLocker-geschützte Laufwerke speichern können, die von anderen Organisationen konfiguriert wurden. Welche der folgenden Richtlinien müssen Sie konfigurieren? (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)

   A. *Verwendung von BitLocker auf Wechseldatenträgern steuern*

   B. *BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern*

   C. *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind*

   D. *Eindeutige IDs für Ihre Organisation angeben*

3. Welche der folgenden Richtlinien müssen Sie konfigurieren, damit ein Computer ohne TPM-Chip unter Windows 7 Enterprise sein Festplattenlaufwerk mit BitLocker schützen kann?

   A. *Zusätzliche Authentifizierung beim Start anfordern*

   B. *Erweiterte PINs für Systemstart zulassen*

   C. *TPM-Plattformvalidierungsprofil konfigurieren*

   D. *Minimale PIN-Länge für Systemstart konfigurieren*

4. Welche der folgenden BitLocker-Richtlinien sollten Sie konfigurieren, damit auf allen mit FAT formatierten und mit BitLocker geschützten Wechseldatenträgern das BitLocker To Go-Lesetool verfügbar ist?

   A. *Kennwortverwendung für Wechseldatenträger konfigurieren*

   B. *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen*

   C. *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können*

   D. *Verwendung von BitLocker auf Wechseldatenträgern steuern*

5. Mit welchem der folgenden Tools können Sie überprüfen, welche Kennung einem mit BitLocker geschützten Volume im ID-Feld zugewiesen wurde?

   A. *Manage-bde.exe*

   B. *Cipher.exe*

   C. *Bcdedit.exe*

   D. *Sigverif.exe*

Lektion 2: Windows 7 und Mobilität

Durch eine fachgemäße Einstellung der Energieoptionen lässt sich der Stromverbrauch einer Organisation deutlich reduzieren, vor allem wenn viele Computer im Einsatz sind. Verbesserungen in der Energiesteuerung von Windows 7 bedeuten, dass der Wechsel von Windows XP auf Windows 7 den Energieverbrauch senken kann. Das kann für eine Organisation zwei wichtige Vorteile haben: sie schadet der Umwelt weniger und die Stromrechnung ist niedriger.

Offlinedateien sind zwischengespeicherte Kopien von Dateien, die in freigegebenen Ordnern liegen. Sie sind insbesondere für mobile Computer wichtig, denn sie ermöglichen auch dann den Zugriff auf die entsprechenden Daten, wenn der Mobilcomputer nicht mehr mit dem Büronetzwerk verbunden ist. Nachdem der Computer wieder mit dem Büronetzwerk verbunden ist, wird der Offline-Inhalt synchronisiert. Dabei werden die Inhalte auf den Servern und Clients nach Bedarf aktualisiert.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Verwalten von Offlinedateien
- Verwalten der Energieoptionen von Windows 7
- Konfigurieren der Energieverwaltungsrichtlinien von Windows 7

Veranschlagte Zeit für diese Lektion: 40 Minuten

Offlinedateien

Die Offlinedateifunktion von Windows 7 ermöglicht es Clients, Dateien aus freigegebenen Ordnern lokal zwischenzuspeichern, damit sie auch dann verfügbar sind, wenn der Computer keine direkte Verbindung mit der Ressource im Netzwerk herstellen kann. Offlinedateien sind in den Windows 7-Editionen Professional, Enterprise und Ultimate verfügbar. Mit Offlinedateien können Sie den Zugang zu den Daten sicherstellen, auch wenn sich ein Clientcomputer nicht mehr im Büro befindet oder die Netzwerkverbindung zwischen einer Zweigstelle und der Zentrale mit ihren freigegebenen Ordnern gestört ist.

Wenn ein Benutzer eine Datei für den Offlinezugriff freigibt, speichert Windows 7 eine Kopie der Datei in einem lokalen Zwischenspeicher. Sollte der Dateiserver, auf dem die Datei liegt, nicht mehr verfügbar sein, weil er zum Beispiel nicht mehr am Netz ist, kann der Benutzer mit der Datei aus dem lokalen Zwischenspeicher weiterarbeiten. Sobald der Dateiserver, auf dem das Original der Datei liegt, wieder verfügbar ist, synchronisiert Windows 7 die Kopie aus dem lokalen Zwischenspeicher mit dem Original aus dem freigegebenen Ordner. Ein Benutzer kann eine Datei offline verfügbar machen, indem er die Datei mit der rechten Maustaste anklickt und dann auf den Menüpunkt *Immer offline verfügbar* klickt (Abbildung 11.17). Ist der Zwischenspeicher für Offlinedateien voll, werden die Dateien gelöscht, die am längsten nicht mehr benutzt wurden, um Platz für neue Dateien zu schaffen. Manuell zwischengespeicherte Dateien löscht Windows 7 nicht, solange der Benutzer diese Dateien nicht löscht.

Offline verfügbare Dateien werden im Windows-Explorer mit dem Status *Immer verfügbar* angezeigt. Abbildung 11.18 zeigt eine Datei namens *Brisbane*, die offline verfügbar ist. Wenn ein Benutzer eine Datei ändert, die offline verfügbar ist, erfolgt eine Synchronisation dieser Datei mit ihrem Original im freigegebenen Ordner, sobald wieder eine Netzwerkverbindung besteht. Dann ersetzt die geänderte Datei das Original im freigegebenen Ordner.

Wurde die Version im freigegebenen Ordner geändert, die Kopie im lokalen Zwischenspeicher aber nicht, wird bei der Synchronisation die Kopie im lokalen Zwischenspeicher überschrieben. Wurden die Datei im freigegebenen Ordner und die Kopie im lokalen Zwischenspeicher beide geändert, muss der Konflikt im Synchronisierungscenter gelöst werden. Über die Verwendung des Synchronisierungscenters erfahren Sie mehr im Verlauf dieser Lektion.

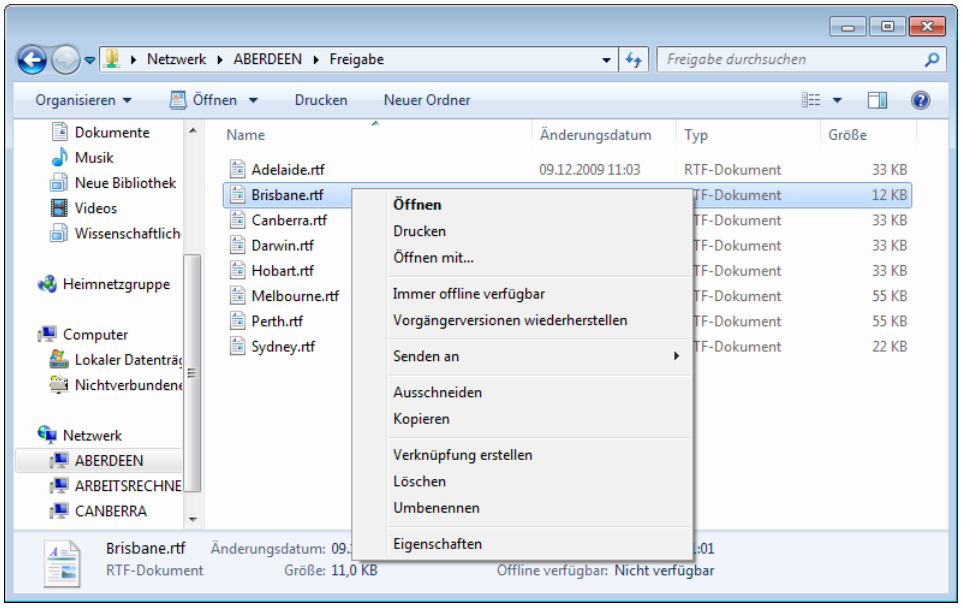


Abbildung 11.17 Eine Datei offline verfügbar machen

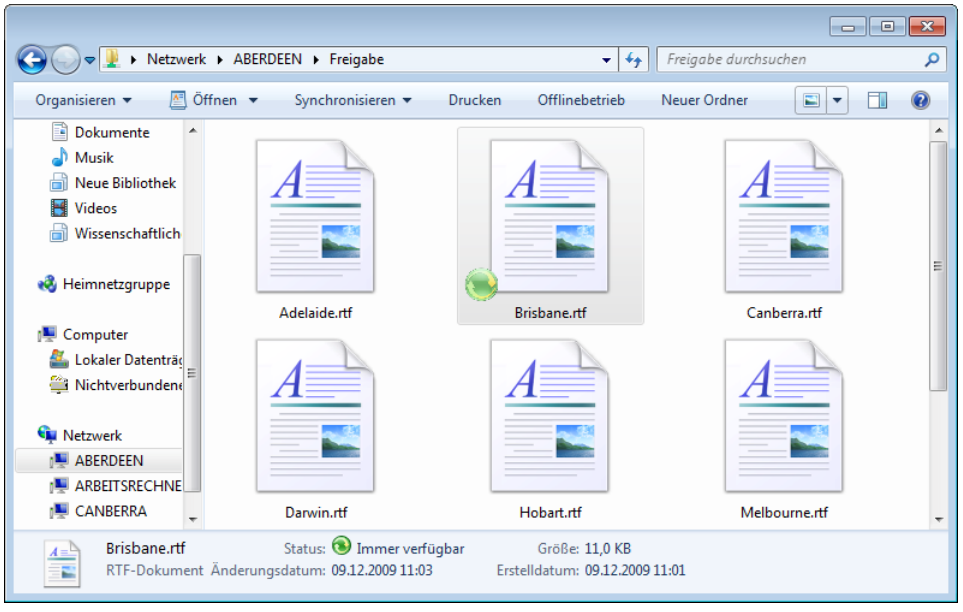


Abbildung 11.18 Die Datei *Brisbane* ist immer verfügbar

Für Offlinedateien bietet Windows 7 vier verschiedene Betriebsarten:

- **Onlinemodus** Änderungen an der Datei werden zuerst in der Dateifreigabe gespeichert und dann in den lokalen Zwischenspeicher übernommen. Die Synchronisation erfolgt automatisch und Benutzer können eine Synchronisation manuell einleiten. Das ist die Standardbetriebsart.
- **Automatischer Offlinemodus** Wird ein Netzwerkfehler erkannt, wechselt Windows 7 in den automatischen Offlinemodus. Dateioperationen erfolgen an der Kopie im lokalen Zwischenspeicher. Windows 7 versucht automatisch alle 2 Minuten, wieder eine Verbindung herzustellen. Kommt eine Verbindung zustande, wechselt Windows 7 wieder in den Onlinemodus.
- **Manueller Offlinemodus** Der Wechsel in den Offlinemodus erfolgt, wenn ein Benutzer im Windows-Explorer auf die Schaltfläche *Offlinebetrieb* klickt. Soll der Computer wieder in den Onlinemodus wechseln, muss im Windows-Explorer ein Klick auf *Onlinebetrieb* erfolgen.
- **Modus für langsame Verbindungen** Dieser Modus ist unter Windows 7 standardmäßig aktiviert und wird wirksam, wenn die Übertragungsrate im Netzwerk unter den Standardwert von 64.000 Bits pro Sekunde fällt. Dieser Wert lässt sich in den Gruppenrichtlinien ändern. In diesem Modus werden Dateioperationen an den Kopien im lokalen Zwischenspeicher durchgeführt. Benutzer können zwar manuell eine Synchronisierung einleiten, aber eine automatische Synchronisierung findet nicht statt. Windows 7 wechselt wieder in den Onlinemodus, wenn die Übertragungsrate den eingestellten Schwellenwert überschreitet.

Im Offlinemodus und im automatischen Offlinemodus sind einige Funktionen nicht verfügbar, beispielsweise Vorgängerversionen, mit denen sich ältere Versionen einer Datei aus Schattenkopien vom Server abrufen lassen.

Richtlinien für Offlinedateien

Offlinedateien lassen sich mit den Gruppenrichtlinien im Knoten *Computerkonfiguration\Administrative Vorlagen\Netzwerk\Offlinedateien* konfigurieren. Es gibt 28 Richtlinien, von denen einige in Abbildung 11.19 zu sehen sind.

Zu den wichtigen Richtlinien, die in diesem Knoten verfügbar sind, gehören:

- **Vom Administrator zugewiesene Offlinedateien** Listet alle Netzwerkdateien und -ordner auf, die ohne Eingreifen von Benutzern für eine Offlineverwendung zur Verfügung stehen.
- **Hintergrundsynchronisierung konfigurieren** Diese Richtlinie gilt für den Modus für langsame Verbindungen und legt fest, wie oft eine Hintergrundsynchronisierung stattfindet.
- **Maßnahme bei nicht standardmäßiger Serververbindungstrennung** Legt fest, ob der Computer automatisch in den Offlinemodus wechselt, wenn er erkennt, dass keine Verbindung mehr zu den Offlinedateiservern besteht.
- **Offlinedateicache verschlüsseln** Legt fest, ob der Offlinedateizwischenspeicher verschlüsselt wird.
- **Modus für langsame Verbindungen konfigurieren** Ermöglicht dem Computer den Wechsel in den Modus für langsame Verbindungen (unter Windows 7 standardmäßig aktiviert).

- **Übertragungsrate für langsame Verbindungen konfigurieren** Legt den Schwellenwert für die Übertragungsrate fest, ab der ein Netzwerk als langsam gilt.

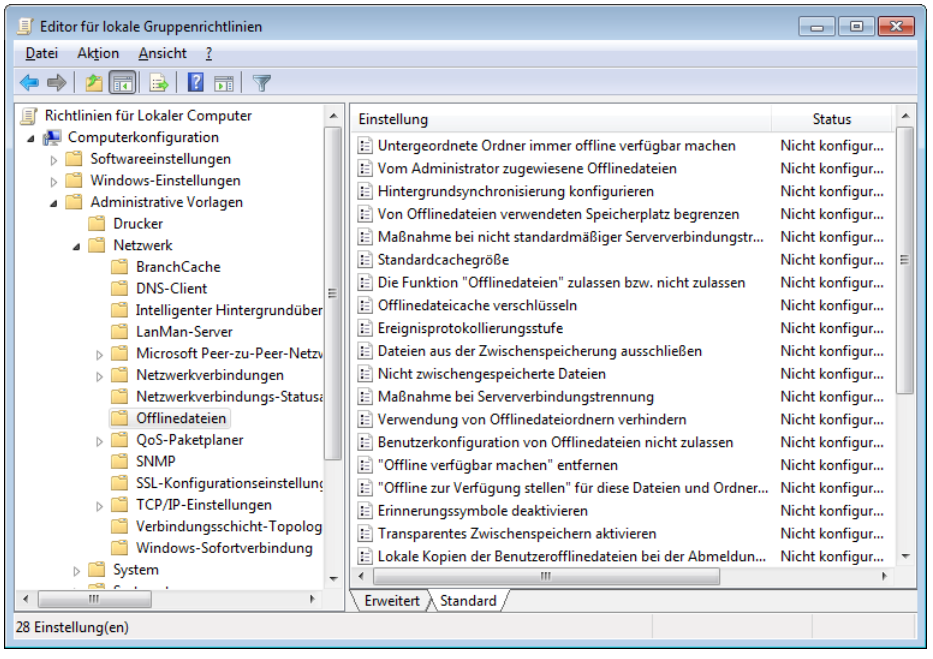


Abbildung 11.19 Richtlinien für Offlinedateien

Transparente Zwischenspeicherung

Wenn Sie die transparente Zwischenspeicherung aktivieren, speichert Windows 7 eine Kopie aller Dateien, die ein Benutzer in einem freigegebenen Ordner öffnet, auf dem lokalen Volume zwischen. Öffnet der Benutzer eine Datei das erste Mal, wird die Datei in den lokalen Zwischenspeicher aufgenommen. Öffnet er sie erneut, überprüft Windows 7, ob die lokal zwischengespeicherte Kopie auf dem neusten Stand ist. Ist dies der Fall, wird diese Kopie verwendet. Ist die Kopie nicht auf dem neusten Stand, öffnet der Client das Original im freigegebenen Ordner und überträgt es erneut in den lokalen Zwischenspeicher. Die Verwendung einer lokal zwischengespeicherten Kopie beschleunigt den Zugriff auf Dateien, die auf Remoteservern gespeichert sind. Wenn ein Benutzer eine Datei ändert, schreibt der Client die Änderung in die Kopie, die sich im lokalen Zwischenspeicher befindet, statt in das Original im freigegebenen Ordner. Wenn der freigegebene Ordner nicht verfügbar ist, ist auch die transparent zwischengespeicherte Kopie nicht verfügbar. Die transparente Zwischenspeicherung versucht nicht, die lokale Kopie synchron zum Original auf dem Remoteserver zu halten, wie es bei Offlinedateien üblich ist. Die transparente Zwischenspeicherung funktioniert bei allen Dateien aus einem freigegebenen Ordner, nicht nur bei denjenigen, die offline verfügbar sein sollen.

Die transparente Zwischenspeicherung eignet sich für WAN-Szenarien und weist eine gewisse Ähnlichkeit mit dem Feature *BranchCache* auf, das in Kapitel 8 beschrieben wurde. Zu den wichtigen Unterschieden gehört, dass Clients aus dem lokalen Netzwerk den Zwischenspeicher nicht gemeinsam verwenden und dass auf den Dateiservern, auf denen die freigegebenen Ordner liegen, nicht Windows Server 2008 R2 verwendet werden muss, um

die transparente Zwischenspeicherung zu unterstützen. Außerdem lässt sich die transparente Zwischenspeicherung auf Clients verwenden, auf denen Windows 7 Professional eingesetzt wird, sowie auf Clients, die keine Domänenmitglieder sind. Das ist bei BranchCache beides nicht möglich. Windows 7 löst eine transparente Zwischenspeicherung aus, wenn die Round-trip-Netzwerklatenz den Schwellenwert überschreitet, der in der Richtlinie *Transparentes Zwischenspeichern aktivieren* festgelegt wurde (Abbildung 11.20).



Weitere Informationen **Transparente Zwischenspeicherung**

Weitere Informationen über die transparente Zwischenspeicherung unter Windows 7 finden Sie auf der folgenden Microsoft TechNet-Webseite: *http://technet.microsoft.com/en-us/library/dd637828.aspx*.

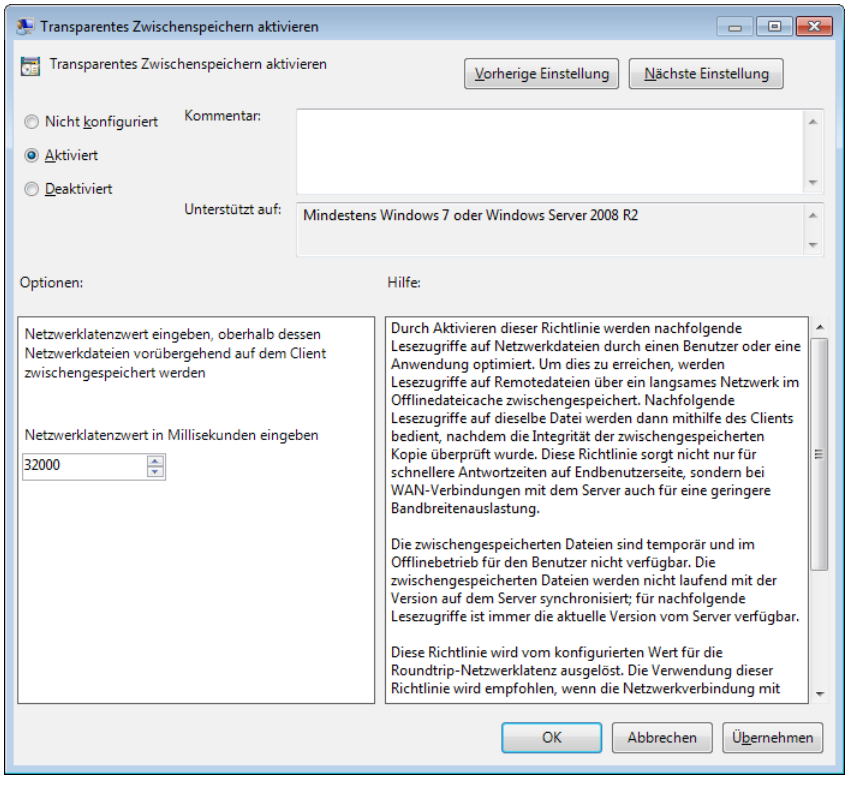

Transparentes Zwischenspeichern aktivieren
Transparentes Zwischenspeichern aktivieren
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows 7 oder Windows Server 2008 R2
Optionen:
Hilfe:
Netzwerklatenzwert eingeben, oberhalb dessen Netzwerkdateien vorübergehend auf dem Client zwischengespeichert werden
Netzwerklatenzwert in Millisekunden eingeben
32000
Durch Aktivieren dieser Richtlinie werden nachfolgende Lesezugriffe auf Netzwerkdateien durch einen Benutzer oder eine Anwendung optimiert. Um dies zu erreichen, werden Lesezugriffe auf Remotedateien über ein langsames Netzwerk im Offlinedateicache zwischengespeichert. Nachfolgende Lesezugriffe auf dieselbe Datei werden dann mithilfe des Clients bedient, nachdem die Integrität der zwischengespeicherten Kopie überprüft wurde. Diese Richtlinie sorgt nicht nur für schnellere Antwortzeiten auf Endbenutzerseite, sondern bei WAN-Verbindungen mit dem Server auch für eine geringere Bandbreitenauslastung.
Die zwischengespeicherten Dateien sind temporär und im Offlinebetrieb für den Benutzer nicht verfügbar. Die zwischengespeicherten Dateien werden nicht laufend mit der Version auf dem Server synchronisiert; für nachfolgende Lesezugriffe ist immer die aktuelle Version vom Server verfügbar.
Diese Richtlinie wird vom konfigurierten Wert für die Roundtrip-Netzwerklatenz ausgelöst. Die Verwendung dieser Richtlinie wird empfohlen, wenn die Netzwerkverbindung mit
OK
Abbrechen
Übernehmen

Abbildung 11.20 Die Richtlinie *Transparentes Zwischenspeichern aktivieren*

Offlinedateiausschlüsse

Administratoren können in den Richtlinien für Offlinedateien bestimmte Dateitypen ausschließen, die dadurch nicht mehr offline verfügbar sind. Verwenden Sie zu diesem Zweck die Richtlinie *Dateien aus der Zwischenspeicherung ausschließen* (Abbildung 11.21). Dateitypen werden in der Richtlinie durch ihre Dateinamenerweiterungen angegeben. Um beispielsweise alle Windows Bitmap-Dateien zu sperren, geben Sie den Dateityp in der Form **.bmp* an. Wenn Sie diese Richtlinie aktivieren, können Benutzer in Ordnern, die offline verfügbar sind, keine Dateien der entsprechenden Typen mehr erstellen.

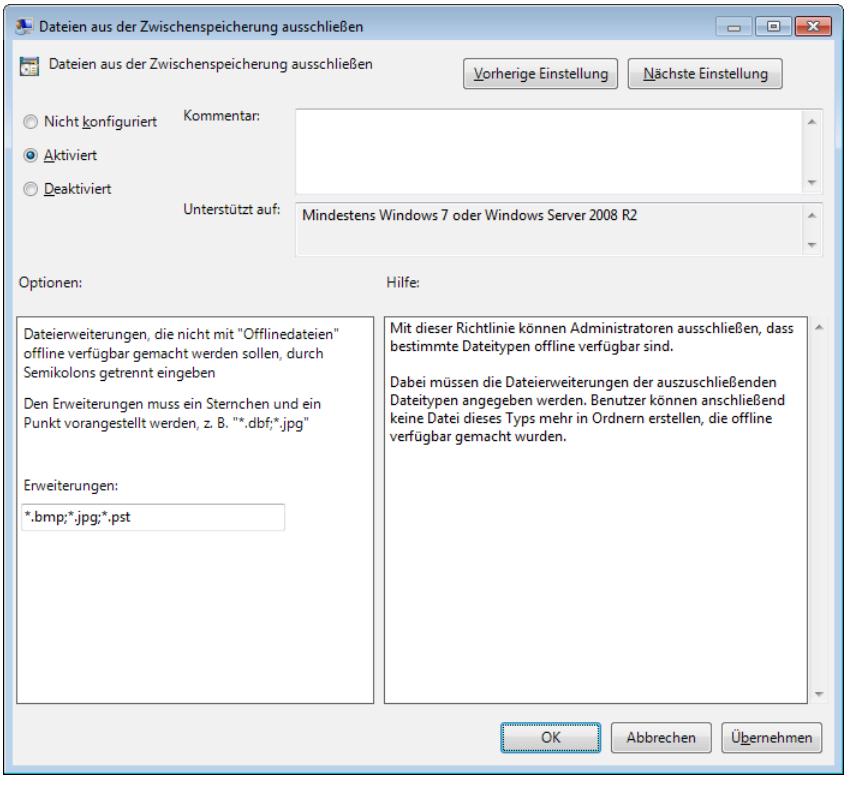

Dateien aus der Zwischenspeicherung ausschließen
Dateien aus der Zwischenspeicherung ausschließen
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows 7 oder Windows Server 2008 R2
Optionen:
Hilfe:
Dateierweiterungen, die nicht mit "Offlinedateien" offline verfügbar gemacht werden sollen, durch Semikolons getrennt eingeben
Den Erweiterungen muss ein Sternchen und ein Punkt vorangestellt werden, z. B. "*.dbf;*.jpg"
Erweiterungen:
.bmp;.jpg;*.pst
Mit dieser Richtlinie können Administratoren ausschließen, dass bestimmte Dateitypen offline verfügbar sind.
Dabei müssen die Dateierweiterungen der auszuschließenden Dateitypen angegeben werden. Benutzer können anschließend keine Datei dieses Typs mehr in Ordnern erstellen, die offline verfügbar gemacht wurden.
OK
Abbrechen
Übernehmen

Abbildung 11.21 Offlinedateiausschlüsse

Verwenden des Synchronisierungscenters

Sie können das Synchronisierungscenter verwenden, um Dateien zu synchronisieren, Offlinedateien zu verwalten und Synchronisationskonflikte manuell zu lösen. Sie finden das Synchronisierungscenter in der Systemsteuerung oder durch die Eingabe von **Synchronisierungscenter** im Textfeld *Programme/Dateien durchsuchen* des *Start*-Menüs. Ein Klick auf *Offlinedateien verwalten* öffnet das Dialogfeld *Offlinedateien* (Abbildung 11.22). In diesem Dialogfeld können Sie Offlinedateien deaktivieren, Offlinedateien anzeigen, die Datenträgerverwendung und die Verschlüsselung für Offlinedateien konfigurieren und festlegen, wie oft Windows 7 überprüfen soll, ob die Netzwerkverbindung langsam ist.

Ein Synchronisationskonflikt tritt auf, wenn eine Datei sowohl auf dem Dateiserver als auch im lokalen Zwischenspeicher geändert wurde. Ein Beispiel: Kim Akers hat eine Datei namens *Brisbane.doc* offline verfügbar gemacht. Kim nimmt ihren portablen Computer mit nach Hause und arbeitet über das Wochenende mit der Datei. Sam Abolrous geht am Wochenende ins Büro und arbeitet mit dem Original der Datei *Brisbane.doc*, das auf dem Dateiserver gespeichert ist. Wenn Kim ihren portablen Computer wieder ans Netzwerk anschließt, wird sie vom Synchronisierungscenter darüber informiert, dass ein Synchronisationskonflikt besteht. Kim kann diesen Konflikt zwischen der Datei, die sie zu Hause verwendet hat, und der Datei, die Sam auf dem Dateiserver geändert hat, mit dem Synchronisierungscenter beheben.

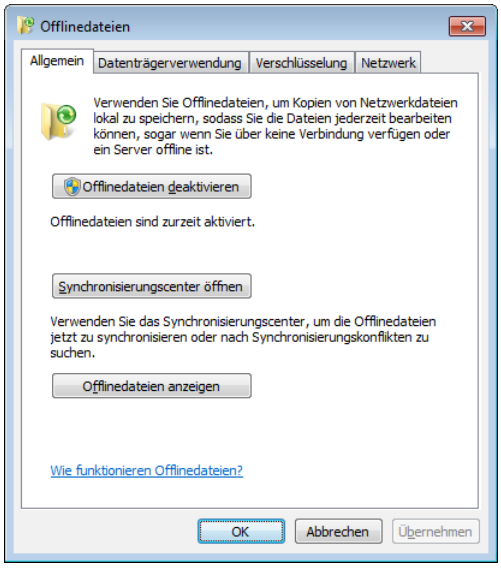

Offlinedateien
Allgemein
Datenträgerverwendung
Verschlüsselung
Netzwerk
Verwenden Sie Offlinedateien, um Kopien von Netzwerkdateien lokal zu speichern, sodass Sie die Dateien jederzeit bearbeiten können, sogar wenn Sie über keine Verbindung verfügen oder ein Server offline ist.
Offlinedateien deaktivieren
Offlinedateien sind zurzeit aktiviert.
Synchronisierungscenter öffnen
Verwenden Sie das Synchronisierungscenter, um die Offlinedateien jetzt zu synchronisieren oder nach Synchronisierungskonflikten zu suchen.
Offlinedateien anzeigen
Wie funktionieren Offlinedateien?
OK
Abbrechen
Übernehmen

Abbildung 11.22 Das Dialogfeld *Offlinedateien*

Wenn Sie im Synchronisierungscenter auf *Synchronisierungskonflikte anzeigen* klicken, sehen Sie eine Liste der Dateien, bei denen ein Synchronisationskonflikt aufgetreten ist (Abbildung 11.23).

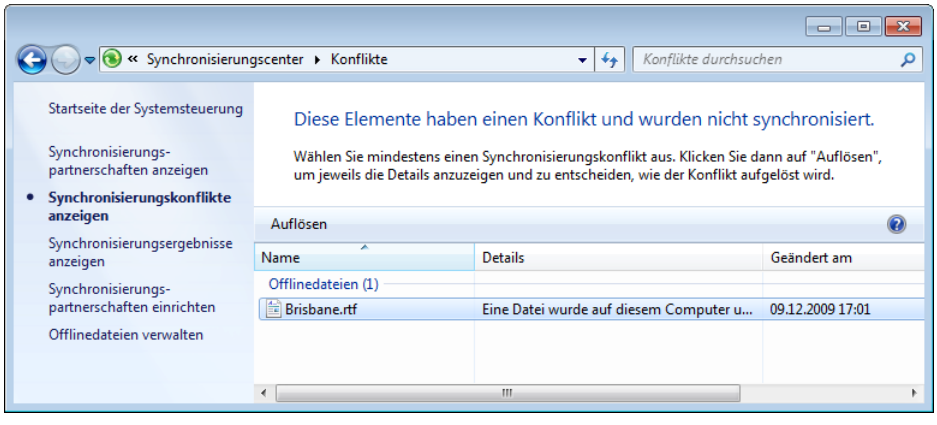


Abbildung 11.23 Anzeigen von Synchronisationskonflikten

Wenn Sie auf der Seite *Konflikte* einen angezeigten Konflikt anklicken und dann auf *Auflösen* klicken, haben Sie die Wahl zwischen drei Aktionen:

- **Die lokale Version behalten** Die auf dem lokalen Computer gespeicherte Version wird beibehalten. Diese Version überschreibt die geänderte Version der Datei, die sich auf der Dateifreigabe befindet.

- **Die Serverversion behalten** Die Version der Datei, die auf der Dateifreigabe gespeichert ist, wird beibehalten. Die Änderungen an der lokalen Version gehen verloren.
- **Beide Versionen behalten** Die Version auf dem lokalen Computer wird umbenannt und dann in der Dateifreigabe gespeichert. Die Version, die sich in der Dateifreigabe befindet, behält ihren ursprünglichen Namen.

Abbildung 11.24 zeigt diese Optionen für das beschriebene Beispiel der geänderten Offlinedatei von Kim Akers.

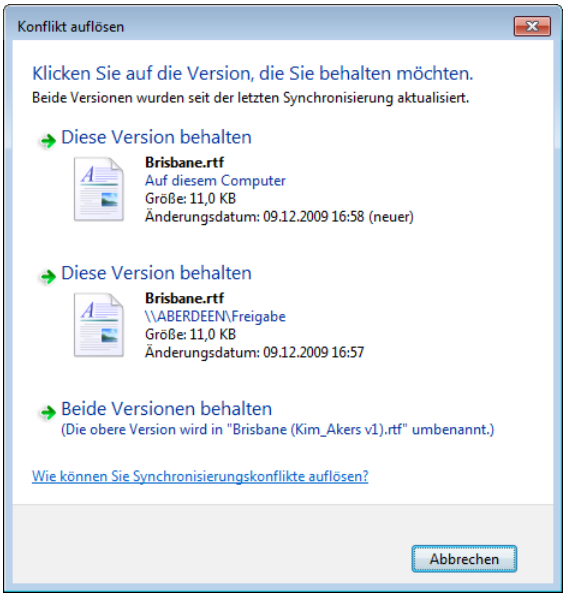


Abbildung 11.24 Auflösen des Konflikts

Konfigurieren eines freigegebenen Ordners für Offlinedateien

Benutzer können Dateien nur dann offline verfügbar machen, wenn der freigegebene Ordner, in dem diese Dateien liegen, Offlinedateien unterstützt. Unter Windows 7 können Sie einen freigegebenen Ordner folgendermaßen für die Unterstützung von Offlinedateien konfigurieren:

1. Öffnen Sie das Eigenschaftendialogfeld des Ordners, den Sie für die Unterstützung von Offlinedateien konfigurieren möchten.
2. Klicken Sie auf der Registerkarte *Freigabe* auf *Erweiterte Freigabe*.
3. Klicken Sie im Dialogfeld *Erweiterte Freigabe* auf *Zwischenspeichern*. Es öffnet sich das Dialogfeld *Offlineeinstellungen* (Abbildung 11.25). In diesem Dialogfeld können Sie festlegen, ob alle Dateien, keine Dateien oder nur die Dateien offline verfügbar sein sollen, die von Benutzern für die Offlineverwendung ausgewählt werden.

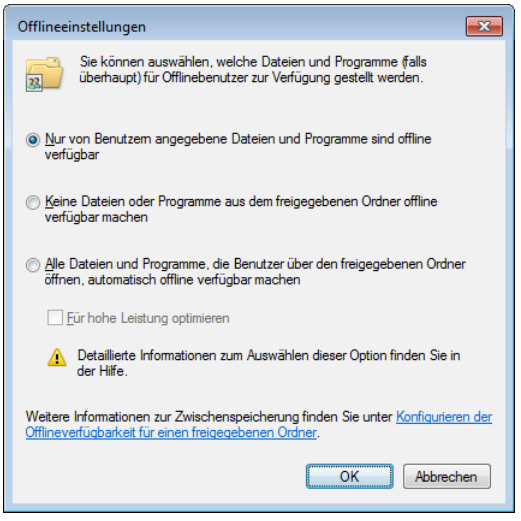

Offlineeinstellungen
Sie können auswählen, welche Dateien und Programme (falls überhaupt) für Offlinebenutzer zur Verfügung gestellt werden.
Nur von Benutzern angegebene Dateien und Programme sind offline verfügbar
Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen
Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen
Für hohe Leistung optimieren
Detaillierte Informationen zum Auswählen dieser Option finden Sie in der Hilfe.
Weitere Informationen zur Zwischenspeicherung finden Sie unter Konfigurieren der Offlineverfügbarkeit für einen freigegebenen Ordner.
OK
Abbrechen

Abbildung 11.25 Konfigurieren der Offlineeinstellungen

Schnelltest

- Was sind die Unterschiede zwischen der transparenten Zwischenspeicherung und BranchCache in Bezug auf freigegebene Ordner aus Remotenetzwerken?

Antwort zum Schnelltest

- Eine transparente Zwischenspeicherung setzt keine Dateiserver voraus, auf denen Windows Server 2008 R2 ausgeführt wird. Der Zwischenspeicher für die transparente Zwischenspeicherung wird nicht von mehreren Benutzern gemeinsam verwendet. Windows 7 Professional unterstützt eine transparente Zwischenspeicherung. Außerdem lässt sich die transparente Zwischenspeicherung auch auf Computern verwenden, die keine Domänenmitglieder sind.

Energieoptionen unter Windows 7

Energiesparpläne sind Sammlungen von Einstellungen, die festlegen, wie ein Computer unter Windows 7 Strom verwendet. Ein neuer Computer unter Windows 7 bietet drei Energiesparpläne mit den Bezeichnungen *Höchstleistung*, *Ausbalanciert* und *Energiesparmodus*. Viele Computerhersteller richten zudem eigene Energiesparpläne für Windows 7 ein, die präzise an die spezielle Hardwarekonfiguration angepasst sein können. Gewöhnlich läuft die Hardware mit dem Energiesparplan *Höchstleistung* mit ihrer maximalen Leistung, aber auch mit dem höchsten Energieverbrauch, während der Plan *Energiesparmodus* die Geräte so konfiguriert, dass sie weniger Energie verbrauchen und eine dementsprechend geringere Leistung erbringen. Im Akkubetrieb weist ein portabler Computer mit dem Energiesparplan *Höchstleistung* im Vergleich zum Energiesparplan *Energiesparmodus* eine kürzere Betriebsdauer auf, bis der Akku leer ist. Den gewünschten Energiesparplan können Sie für einen Windows 7-Client auf der Seite *Energieoptionen* der Systemsteuerung auswählen (Abbildung 11.26). Der Standardenergieplan für einen frisch installierten Windows 7-Client ist *Ausbalanciert*.

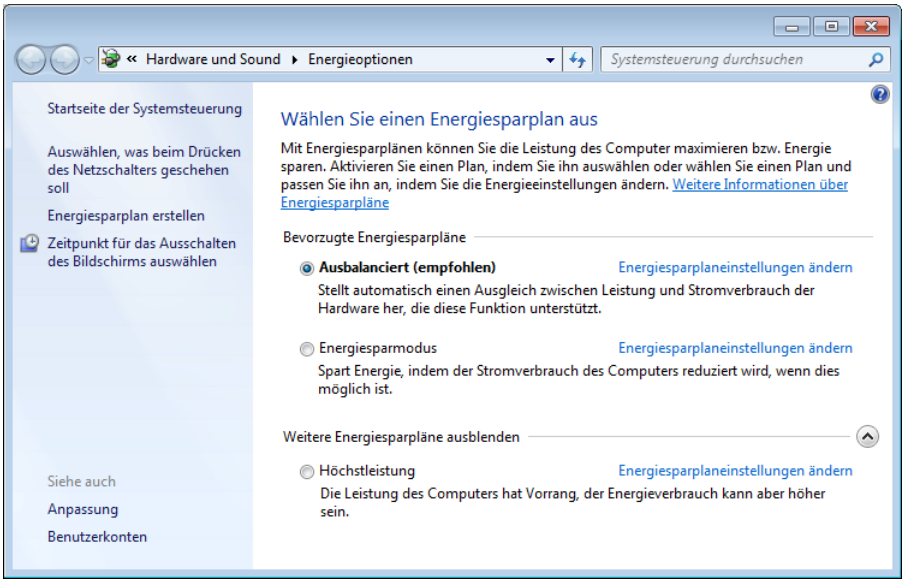

« Hardware und Sound ▸ Energieoptionen
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Auswählen, was beim Drücken des Netzschalters geschehen soll
Energiesparplan erstellen
Zeitpunkt für das Ausschalten des Bildschirms auswählen
Wählen Sie einen Energiesparplan aus
Mit Energiesparplänen können Sie die Leistung des Computer maximieren bzw. Energie sparen. Aktivieren Sie einen Plan, indem Sie ihn auswählen oder wählen Sie einen Plan und passen Sie ihn an, indem Sie die Energieeinstellungen ändern. Weitere Informationen über Energiesparpläne
Bevorzugte Energiesparpläne
Ausbalanciert (empfohlen)
Energiesparplaneinstellungen ändern
Stellt automatisch einen Ausgleich zwischen Leistung und Stromverbrauch der Hardware her, die diese Funktion unterstützt.
Energiesparmodus
Energiesparplaneinstellungen ändern
Spart Energie, indem der Stromverbrauch des Computers reduziert wird, wenn dies möglich ist.
Weitere Energiesparpläne ausblenden
Höchstleistung
Energiesparplaneinstellungen ändern
Die Leistung des Computers hat Vorrang, der Energieverbrauch kann aber höher sein.
Siehe auch
Anpassung
Benutzerkonten

Abbildung 11.26 Auswählen eines Energiesparplans

Windows 7 sieht für jeden Plan Grundeinstellungen und erweiterte Einstellungen vor. Welche Einstellungen im Detail vorgenommen werden können, hängt von der Hardwarekonfiguration des Computers ab. Auf der Seite *Einstellungen für Energiesparplan ändern* (Abbildung 11.27) können Sie die Grundeinstellungen für einen Plan vornehmen. Manche Computer unterstützen auf dieser Seite zum Beispiel auch noch die Einstellungen *Bildschirmhelligkeit regeln* oder *Anzeigehelligkeit anpassen*. In den Grundeinstellungen können Sie für den Akkubetrieb und für den Netzbetrieb unterschiedliche Werte festlegen. Auf Desktopcomputern, die keinen Akkubetrieb vorsehen, können Sie nur Einstellungen für den Netzbetrieb vornehmen.

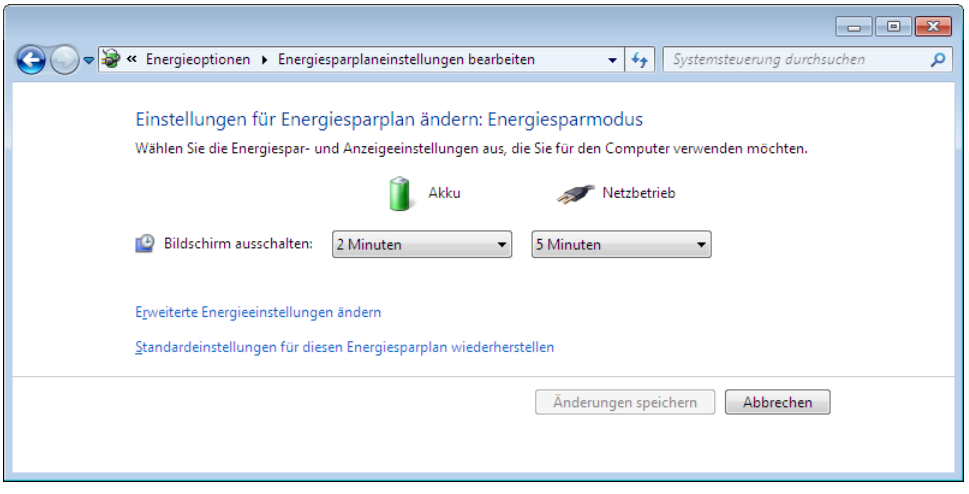


Abbildung 11.27 Die Grundeinstellungen eines Energiesparplans

Ein Benutzer, der kein Mitglied der lokalen Gruppe *Administratoren* ist, kann festlegen, was der Netzschalter und die Energiespartaste bewirken sollen. Wenn er die Rechte anheben kann, kann er auch festlegen, ob beim Hochfahren des Computers aus dem Energiesparmodus ein Kennwort eingegeben werden muss. Diese Optionen können Sie nach einem Klick auf *Auswählen, was beim Drücken von Netzschaltern geschehen soll* konfigurieren, wodurch sich die Seite *Systemeinstellungen* öffnet (Abbildung 11.28). Zur Wahl stehen die Einstellungen *Energie sparen*, *Ruhezustand*, *Herunterfahren* und *Nichts unternehmen*.

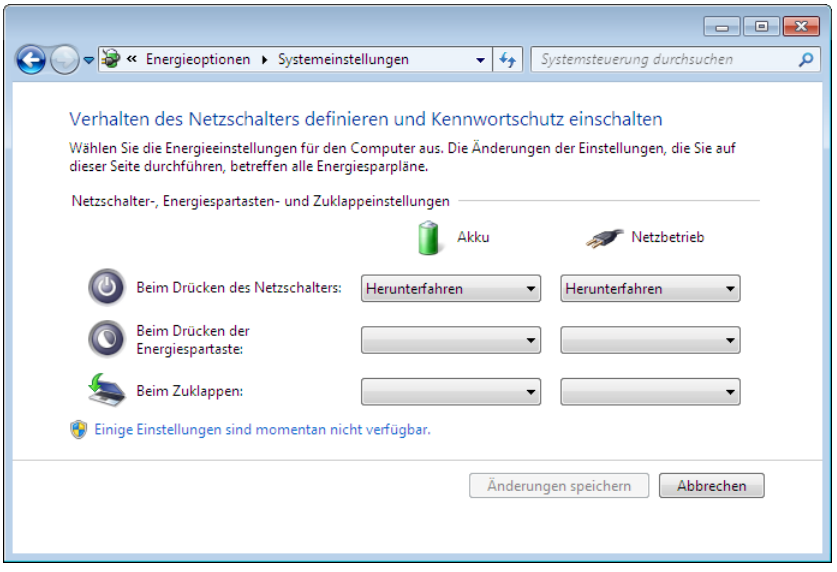

« Energieoptionen ▸ Systemeinstellungen
Systemsteuerung durchsuchen
Verhalten des Netzschalters definieren und Kennwortschutz einschalten
Wählen Sie die Energieeinstellungen für den Computer aus. Die Änderungen der Einstellungen, die Sie auf dieser Seite durchführen, betreffen alle Energiesparpläne.
Netzschalter-, Energiespartasten- und Zuklappeinstellungen
Akku
Netzbetrieb
Beim Drücken des Netzschalters:
Herunterfahren
Herunterfahren
Beim Drücken der Energiespartaste:
Beim Zuklappen:
Einige Einstellungen sind momentan nicht verfügbar.
Änderungen speichern
Abbrechen

Abbildung 11.28 Konfigurieren von Netzschalter und Energiespartaste

Windows 7 unterstützt folgende Modi:

- **Energiesparmodus** Wenn sich Windows 7 im Energiesparmodus befindet, sind der Prozessor und der größte Teil der Systemgeräte ausgeschaltet. Das RAM des Computers bleibt eingeschaltet, damit die darin befindlichen geöffneten Anwendungen und Dokumente erhalten bleiben. Geräte, die den Computer aus dem Energiesparmodus heraus aktivieren können, wie USB-Mäuse, Tastaturen und Netzwerkkarten, bleiben ebenfalls eingeschaltet. Wenn der Computer nach einer einstellbaren Zeitspanne nicht hochgefahren wird, wechselt er in den Ruhezustand. Sie können einen Computer mit der Tastatur oder der Maus aus dem Energiesparmodus heraus aktivieren.
- **Hybrider Energiesparmodus** Der hybride Energiesparmodus soll den Stromverbrauch von Desktopcomputern senken, die nicht über eine ausfallsichere Stromversorgung verfügen. Wenn sich ein Desktopcomputer im Energiesparmodus befindet und in seiner Stromversorgung eine Unterbrechung auftritt, können sich Datenverluste ergeben. Der Inhalt des RAMs, das sich in einem speziellen Ruhezustand mit niedrigem Stromverbrauch befindet, bleibt erhalten und wird zusätzlich als spezielle Datei auf der Festplatte gespeichert. Wenn der hybride Energiesparmodus aktiviert ist, verwenden die Computer nicht den gewöhnlichen Energiesparmodus, sondern den hybriden Energiesparmodus.

- **Ruhezustand** Wenn sich Windows 7 im Ruhezustand befindet, sind alle Geräte ausgeschaltet und der Inhalt des RAMs wurde in einer speziellen Datei auf dem Betriebssystemvolume gespeichert. Alle Geräte sind ausgeschaltet. Einen Computer, der sich im Ruhezustand befindet, können Sie nur mit dem Netzschalter einschalten.
- **Herunterfahren** Wenn der Computer heruntergefahren wird, bleibt der aktuelle Inhalt des RAMs nicht erhalten. Alle Geräte werden ausgeschaltet.



Weitere Informationen Windows 7 Energieverwaltung

Weitere Informationen über die Energieverwaltungsfunktionen von Windows 7, einschließlich der Aktivierung über das Netzwerk, finden Sie in dem folgenden Microsoft TechNet-Artikel: *http://technet.microsoft.com/de-de/library/dd744300(WS.10).aspx*.

Erweiterte Energieeinstellungen

Zur Konfiguration der erweiterten Energieeinstellungen klicken Sie auf der Seite *Einstellungen für Energiesparplan ändern* auf das Element *Erweiterte Energieeinstellungen ändern*. Im Gegensatz zu den Grundeinstellungen, die auch von Benutzern vorgenommen werden können, die nicht Mitglieder der lokalen Gruppe *Administratoren* sind, können nur Benutzer mit erhöhten Rechten die erweiterten Energieeinstellungen ändern (Abbildung 11.29).

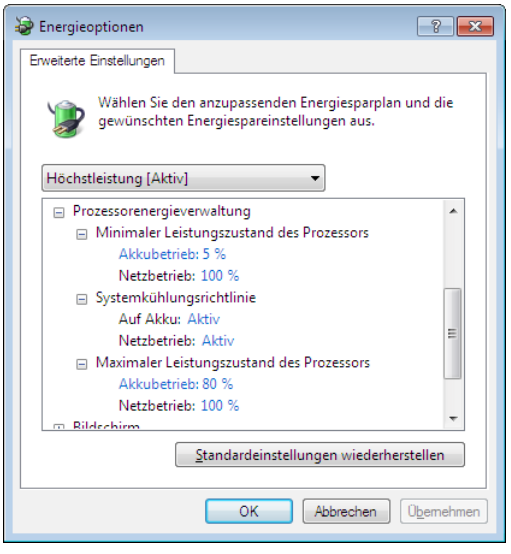


Abbildung 11.29 Erweiterte Energieeinstellungen

Im Dialogfeld *Energieoptionen* für die erweiterten Energieeinstellungen können Sie folgende Einstellungen für Akku- und Netzbetrieb vornehmen:

- **Kennwort bei Reaktivierung anfordern** Legt fest, ob bei der Aktivierung aus dem Energiesparmodus oder Ruhezustand ein Kennwort eingegeben werden muss.
- **Festplatte ausschalten nach** Gibt die Zeitdauer an, nach der das Festplattenlaufwerk ausgeschaltet werden soll.

- **Desktophintergrundeinstellungen** Legt fest, ob im Akku- oder Netzbetrieb animierte Desktophintergründe verfügbar sind, beispielsweise der Diashow-Hintergrund.
- **Drahtlosadaptereinstellungen** Legt die Energieeinstellungen für Drahtlosnetzwerkadapter fest. Zur Verfügung stehen die Einstellungen *Höchstleistung*, *Minimaler Energiesparmodus*, *Mittlerer Energiesparmodus* und *Maximaler Energiesparmodus*. Die verschiedenen Einstellungen beeinflussen die Leistung des Adapters und können sich auf die Reichweite und die Übertragungsgeschwindigkeit auswirken.
- **Energie sparen** Mit dieser Einstellung können Sie Einstellungen für den Wechsel in den Energiesparmodus oder in den Ruhezustand vornehmen. Die Unterschiede zwischen Energiesparmodus, hybridem Energiesparmodus und Ruhezustand wurden in dieser Lektion bereits beschrieben. Folgende Einstellungen sind möglich:
  - **Deaktivierung nach** Legt fest, nach welcher Zeitspanne der Inaktivität der Computer in den Energiesparmodus wechselt.
  - **Hybriden Standbymodus zulassen** Legt fest, ob der Computer den hybriden Energiesparmodus verwenden kann.
  - **Ruhezustand nach** Legt fest, nach welcher Zeitspanne im Energiesparmodus der Computer in den Ruhezustand wechselt.
  - **Zeitgeber zur Aktivierung zulassen** Legt fest, ob der Computer durch einen Zeitgeber aus dem Energiesparmodus heraus aktiviert werden kann.
- **USB-Einstellungen** Legt fest, ob für USB das selektive Energiesparen aktiviert ist.
- **Netzschalter und Zuklappen** Legt fest, was geschehen soll, wenn Sie einfach den Deckel des Laptops zuklappen, auf den Netzschalter drücken oder eine Energiespartaste betätigen. Zu den Optionen zählen *Nichts unternehmen*, *Energie sparen*, *Ruhezustand* und *Herunterfahren*.
- **PCI-Express** Legt fest, ob Windows 7 die Verbindungszustand-Energieverwaltung (PCI Express Link State Power Management) verwenden kann, wenn sich ein Gerät im Leerlauf befindet. Die verfügbaren Einstellungen sind *Aus*, *Mittlere Energieeinsparungen* und *Maximale Energieeinsparungen*.
- **Prozessorenergieverwaltung** Gibt prozentual einen *Minimalen Leistungszustand des Prozessors* und einen *Maximalen Leistungszustand des Prozessors* an. Es lässt sich auch festlegen, ob die Systemkühlungsrichtlinie aktiv ist.
- **Bildschirm** Legt fest, nach welcher Zeitspanne der Bildschirm abgeblendet und nach welcher Zeitspanne er ausgeschaltet werden soll. Es ist auch möglich, die normale Bildschirmhelligkeit und die Helligkeit des abgeblendeten Bildschirms festzulegen.
- **Multimediaeinstellungen** Dieser Abschnitt ermöglicht folgende Einstellungen:
  - **Bei der Freigabe von Medien** Legt fest, wie der Computer auf Medienzugriffe durch Remotecomputer reagiert. Möglich sind die Einstellungen, in den Energiesparmodus zu wechseln, den Wechsel in den Energiesparmodus bei Inaktivität zu verhindern und den Wechsel in den Modus »Abwesend« zuzulassen.
  - **Bei der Videowiedergabe** Die möglichen Einstellungen sind *Videoqualität optimieren*, *Ausbalanciert* und *Energieeinsparung optimieren*.

- **Batterie** Legt prozentual die Ladezustände für die Einstufungen Reserve, niedrig und kritisch an. Es lässt sich auch festlegen, was geschehen soll, wenn die Ladezustände niedrig oder kritisch erreicht werden. Möglich sind die Einstellungen *Nichts unternehmen*, *Energie sparen*, *Ruhezustand* und *Herunterfahren*.

Wenn die drei Energiesparpläne nicht Ihren Anforderungen genügen, können Sie einen passenden benutzerdefinierten Energiesparplan erstellen. Dazu klicken Sie auf der Seite *Energieoptionen* der Systemsteuerung auf *Energiesparplan erstellen*. Einen benutzerdefinierten Energiesparplan können Sie auch wieder löschen, sofern er nicht der aktive Energiesparplan ist. Die vordefinierten Standardenergiesparpläne lassen sich nicht löschen. In der Übung am Ende dieser Lektion erstellen Sie einen benutzerdefinierten Energiesparplan.

Gruppenrichtlinien für die Energieverwaltung

Die Gruppenrichtlinien für die Energieverwaltung liegen im Knoten *Computerkonfiguration\Administrative Vorlagen\System\Energieverwaltung*. Der Knoten enthält fünf weitere Knoten (Abbildung 11.30).

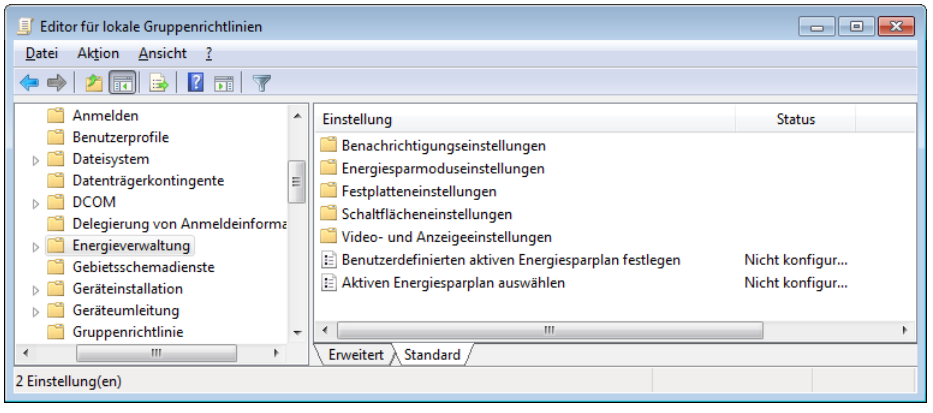


Abbildung 11.30 Gruppenrichtlinien für die Energieverwaltung

Mit diesen Richtlinien können Sie alle Einstellungen vornehmen, die in diesem Kapitel bereits im Abschnitt »Erweiterte Energieeinstellungen« beschrieben wurden. Außerdem gibt es im Knoten *Energiesparmoduseinstellungen* einige zusätzliche Richtlinien, mit denen Einstellungen möglich sind, die sich nur in den Gruppenrichtlinien konfigurieren lassen. Dazu gehören:

- *Verhindern des automatischen Energiesparmodus für Anwendungen zulassen*
- *Automatischen Energiesparmodus bei geöffneten Netzwerkdateien zulassen*
- *Wechsel in den Energiesparmodus durch Anwendungen verhindern*

Jede dieser Richtlinien hat damit zu tun, ob Anwendungen oder offene Netzwerkdateien einen Computer daran hindern können, automatisch in den Energiesparmodus zu wechseln. Wenn diese Richtlinien deaktiviert sind, werden nur direkte Eingaben des Benutzers für die Beurteilung herangezogen, ob die Leerlaufphase für einen Wechsel in den Energiesparmodus bereits lang genug war. Diese Richtlinien haben keine Wirkung, wenn der Benutzer den Computer manuell in den Energiesparmodus versetzt.

Energieverwaltung auf der Befehlszeile

Powercfg.exe ist ein Befehlszeilenprogramm, mit dem Sie in einer Eingabeaufforderung mit erhöhten Rechten unter Windows 7 Energieeinstellungen vornehmen können. Mit *Powercfg.exe* lassen sich auch einige Einstellungen für Windows 7 vornehmen, die weder in den Gruppenrichtlinien noch im Dialogfeld *Energieoptionen* mit den erweiterten Energieeinstellungen möglich sind. Sie können mit *Powercfg.exe* bestimmte Geräte so konfigurieren, dass sie den Computer aus dem Energiesparmodus heraus aktivieren können. Mit den Import- und Exportfunktionen von *Powercfg.exe* können Sie auch Energieverwaltungsrichtlinien von einem Windows 7-Computer auf einen anderen übertragen. Tabelle 11.2 beschreibt einige Optionen von *Powercfg.exe*.

Tabelle 11.2 *Powercfg.exe*-Optionen

Option	Beschreibung
`-list`	Listet alle verfügbaren Energieschemas auf.
`-query <Schema_GUID>`	Zeigt den Inhalt des angegebenen Energieschemas an.
`-change`	Dient zum Ändern einer bestimmten Einstellung im aktuellen Energieschema.
`-hibernate`	Aktiviert oder deaktiviert die Funktion »Ruhezustand«.
`-devicequery <Option>`	Listet Geräte auf, die den Computer aktivieren können: ■ **Wake_From_Any** Listet alle Geräte auf, die es unterstützen, den Computer aus einem Standbymodus zu aktivieren. ■ **Wake_Armed** Listet alle Geräte auf, die den Computer aus jedem Standbymodus aktivieren können.
`-deviceenablewake <Gerätename>`	Ermöglicht es dem Gerät, den Computer aus einem Standbymodus zu aktivieren.
`-devicedisablewake <Gerätename>`	Verhindert, dass das Gerät den Computer aus einem Standbymodus aktivieren kann.
`-import / -export`	Ermöglicht die Übertragung von Energiesparplänen durch Export und Import.
`-lastwake`	Liefert Informationen über das letzte Ereignis, das den Computer aus einem Energiesparmodus reaktiviert hat.
`-requests`	Listet Energieanforderungen von Anwendungen und Treibern auf, die einen Wechsel in einen Energiesparmodus verhindern können.
`-requestsoverride`	Ermöglicht es Ihnen, eine bestimmte Energieanforderung von einer Anwendung oder einem Treiber außer Kraft zu setzen, damit sie nicht mehr den Wechsel des Computers in einen Energiesparmodus verhindert.
`-energy`	Überprüft den Computer auf allgemeine Probleme hinsichtlich Energieeffizienz und Akkuzustand. Erstellt einen Bericht im HTML-Format (Hypertext Markup Language).



Weitere Informationen *Powercfg.exe*

Weitere Informationen über *Powercfg.exe* erhalten Sie in dem folgenden Microsoft TechNet-Dokument: *http://technet.microsoft.com/de-de/library/cc748940.aspx.*



Prüfungstipp

Merken Sie sich, mit welcher Befehlszeilenoption sich ermitteln lässt, welche Hardwaregeräte einen Windows 7-Client aus dem Energiesparmodus reaktivieren können.

Übung Verwalten von Energiesparplänen

Energiesparpläne ermöglichen eine Einstellung der Energieoptionen, die sich optimal für die Anforderungen eignen, die verschiedene Benutzer jeweils an ihre Computer stellen. In dieser Übung erstellen Sie einen benutzerdefinierten Energiesparplan und simulieren dann die Übertragung dieses Plans auf einen anderen Windows 7-Computer.

Übung 1 Erstellen eines benutzerdefinierten Energiesparplans

In dieser Übung erstellen Sie auf der Basis des Energiesparplans *Energiesparmodus* einen benutzerdefinierten Energiesparplan und konfigurieren ihn.

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* am Computer *Canberra* an.
2. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Energieoptionen** ein. Klicken Sie auf das Element *Energieoptionen*, um die Seite *Energieoptionen* der Systemsteuerung zu öffnen.
3. Wählen Sie den Plan *Energiesparmodus* und klicken Sie dann auf *Energiesparplan erstellen*.
4. Wählen Sie auf der Seite *Energiesparplan erstellen* den Plan *Energiesparmodus* und geben Sie dann den benutzerdefinierten Namen **Extrem-Energiesparen** ein (Abbildung 11.31). Klicken Sie auf *Weiter*.

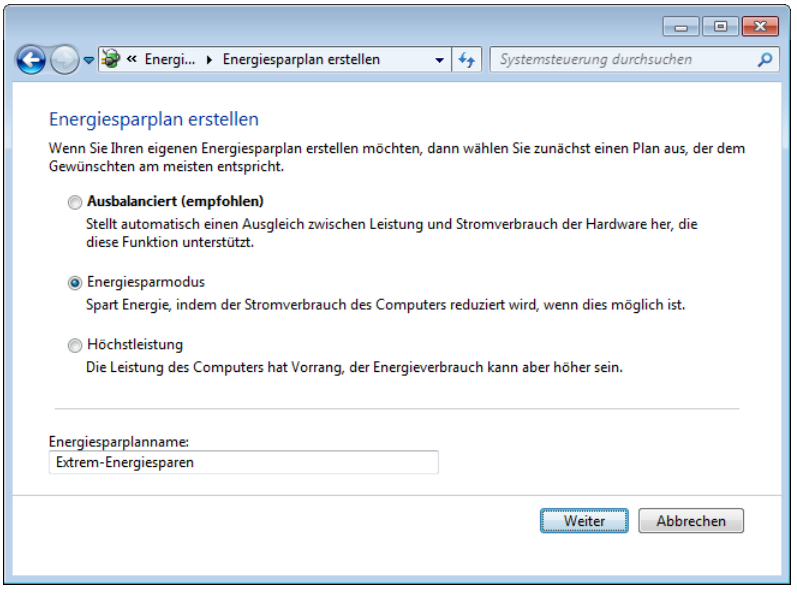

« Energi... ▸ Energiesparplan erstellen
Systemsteuerung durchsuchen
Energiesparplan erstellen
Wenn Sie Ihren eigenen Energiesparplan erstellen möchten, dann wählen Sie zunächst einen Plan aus, der dem Gewünschten am meisten entspricht.
Ausbalanciert (empfohlen)
Stellt automatisch einen Ausgleich zwischen Leistung und Stromverbrauch der Hardware her, die diese Funktion unterstützt.
Energiesparmodus
Spart Energie, indem der Stromverbrauch des Computers reduziert wird, wenn dies möglich ist.
Höchstleistung
Die Leistung des Computers hat Vorrang, der Energieverbrauch kann aber höher sein.
Energiesparplanname:
Extrem-Energiesparen
Weiter
Abbrechen

Abbildung 11.31 Neuer benutzerdefinierter Energiesparplan

5. Klicken Sie auf der Seite *Einstellungen für Energiesparplan ändern: Extrem-Energiesparen* auf *Erstellen*. Auf der Seite *Energieoptionen* klicken Sie auf *Energiesparplaneinstellungen ändern*. Klicken Sie auf der Seite *Einstellungen für Energiesparplan ändern* dann auf *Erweiterte Energieeinstellungen ändern*.
6. Klicken Sie auf der Registerkarte *Erweiterte Einstellungen* des Dialogfelds *Energieoptionen* auf *Zurzeit nicht verfügbare Einstellungen ändern* (Abbildung 11.32).

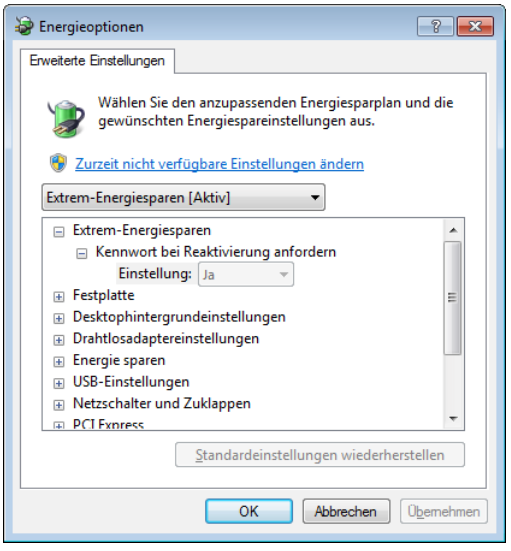


Abbildung 11.32 Die Registerkarte *Erweiterte Einstellungen* des Dialogfelds *Energieoptionen*

7. Ändern Sie die Einstellung *Kennwort bei Reaktivierung anfordern* auf *Nein*.
8. Erweitern Sie den Knoten *Netzschalter und Zuklappen*. Stellen Sie die *Energiespartastenaktion* auf *Ruhezustand*.
9. Erweitern Sie den Knoten *Prozessorenergieverwaltung*. Stellen Sie den *Maximalen Leistungszustand des Prozessors* auf 80 Prozent. Klicken Sie auf *OK*. Schließen Sie die Systemsteuerung.

Übung 2 Migrieren eines Energiesparplans

In dieser Übung exportieren Sie den Plan, den Sie in Übung 1 erstellt haben, mit dem Befehlszeilenprogramm *Powercfg.exe*. Anschließend löschen Sie den erstellten Plan und importieren ihn wieder auf demselben Computer (als Ersatz für den Import auf einem anderen Computer).

1. Verwenden Sie in einer Eingabeaufforderung mit erhöhten Rechten den Befehl **Powercfg.exe -list** ein**.** Die Ausgabe sollte so ähnlich wie in Abbildung 11.33 aussehen, wenn auch mit anderen GUIDs (Globally Unique Identifiers) für die Energieschemas. Notieren Sie sich die GUID des Plans *Extreme-Energiesparen*, denn Sie brauchen diese Kennung für Schritt 4. Sie können die GUID auch markieren und in die Zwischenablage kopieren.

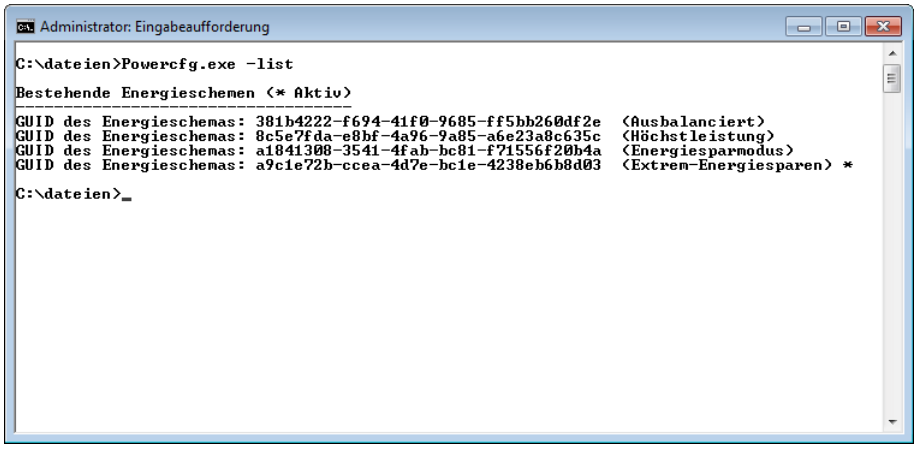


Abbildung 11.33 Auflisten der Energiepläne und GUIDs

2. Erstellen Sie den Ordner *C:\Export*, sofern er noch nicht vorhanden ist. Wechseln Sie in diesen Ordner.
3. Geben Sie den Befehl **Powercfg.exe -energy** ein. Verwenden Sie nach der Ausführung dieses Befehls den Befehl **start energy-report.html**. Dadurch öffnet sich der Internet Explorer mit dem Energiebericht (Abbildung 11.34). Überprüfen Sie den Bericht und schließen Sie dann den Internet Explorer.

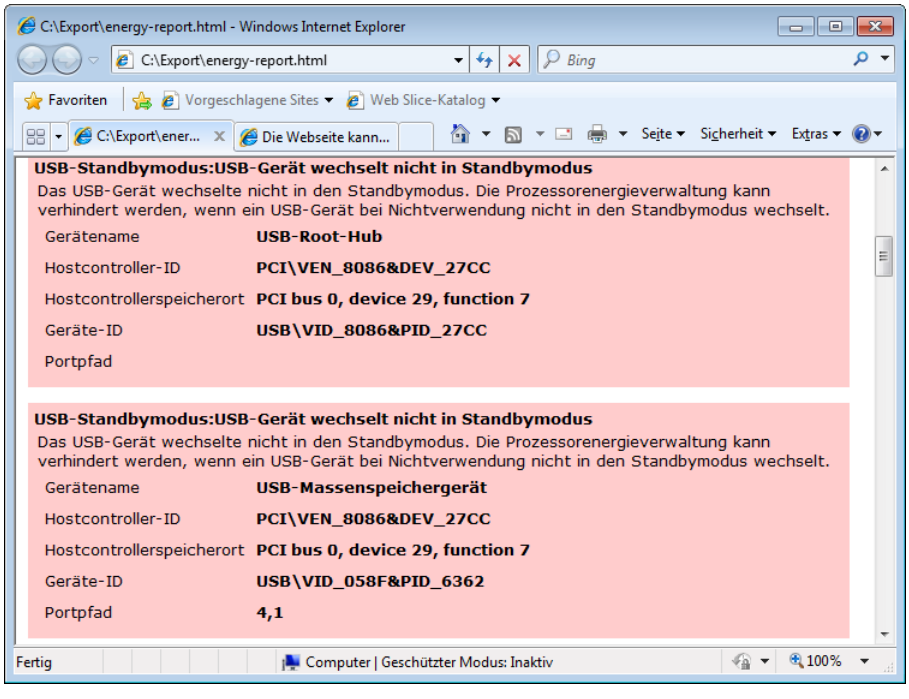

C:\Export\energy-report.html - Windows Internet Explorer
C:\Export\energy-report.html
Bing
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
C:\Export\ener...
Die Webseite kann...
Seite
Sicherheit
Extras
USB-Standbymodus:USB-Gerät wechselt nicht in Standbymodus
Das USB-Gerät wechselte nicht in den Standbymodus. Die Prozessorenergieverwaltung kann verhindert werden, wenn ein USB-Gerät bei Nichtverwendung nicht in den Standbymodus wechselt.
Gerätename USB-Root-Hub
Hostcontroller-ID PCI\VEN_8086&DEV_27CC
Hostcontrollerspeicherort PCI bus 0, device 29, function 7
Geräte-ID USB\VID_8086&PID_27CC
Portpfad
USB-Standbymodus:USB-Gerät wechselt nicht in Standbymodus
Das USB-Gerät wechselte nicht in den Standbymodus. Die Prozessorenergieverwaltung kann verhindert werden, wenn ein USB-Gerät bei Nichtverwendung nicht in den Standbymodus wechselt.
Gerätename USB-Massenspeichergerät
Hostcontroller-ID PCI\VEN_8086&DEV_27CC
Hostcontrollerspeicherort PCI bus 0, device 29, function 7
Geräte-ID USB\VID_058F&PID_6362
Portpfad 4,1
Fertig
Computer | Geschützter Modus: Inaktiv
100%

Abbildung 11.34 Anzeigen des Energieberichts

4. Verwenden Sie den Befehl **Powercfg.exe -export extrem.pow {GUID},** wobei *{GUID}* die GUID des Plans *Extreme-Energiesparen* ist.
5. Verwenden Sie den Befehl **Powercfg.exe -setactive SCHEME_BALANCED.**
6. Überprüfen Sie mit dem Befehl **Powercfg.exe -list**, ob nun das Energieschema *Ausbalanciert* das aktuelle Energieschema ist. Notieren Sie sich die GUID des Plans *Extreme-Energiesparen*.
7. Geben Sie den Befehl **Powercfg.exe -delete {GUID}** ein, wobei *{GUID}* die GUID des Plans *Extreme-Energiesparen* ist.
8. Überprüfen Sie mit dem Befehl **Powercfg.exe -list**, ob der Plan *Extreme-Energiesparen* gelöscht wurde. Es sollten nur noch drei Energieschemas zu sehen sein (Abbildung 11.35).

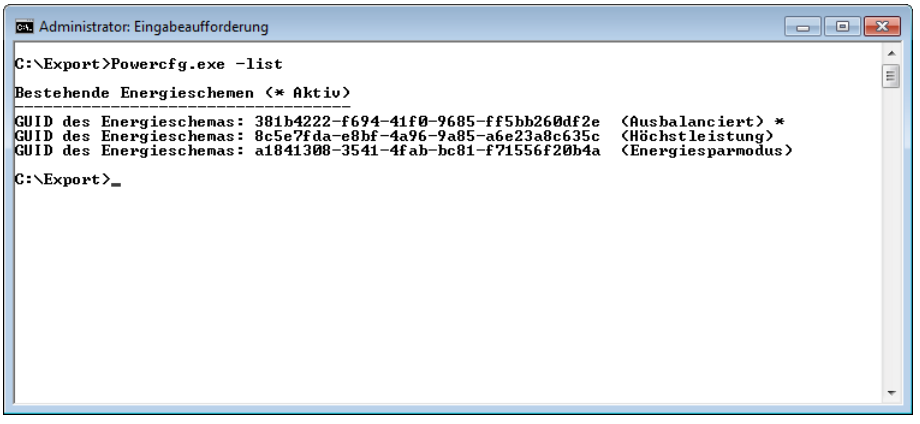


Abbildung 11.35 Überprüfen der Löschung des Energieplans

9. Importieren Sie den zuvor exportierten Plan mit dem Befehl **Powercfg.exe -import c:\export\extrem.pow**.
10. Überprüfen Sie mit dem Befehl **Powercfg.exe -list**, ob das Energieschema tatsächlich importiert wurde. Der Plan *Extreme-Energiesparen* sollte wieder verfügbar sein.

Zusammenfassung der Lektion

- Offlinedateien sind in den Editionen Windows 7 Professional, Enterprise und Ultimate verfügbar und ermöglichen einem Benutzer auch dann die Arbeit mit Dateien aus freigegebenen Ordnern, wenn er nicht mit dem Netzwerk verbunden ist, zu dem der freigegebene Ordner gehört.
- Offlinedateien sind lokal zwischengespeicherte Kopien der Dateien von freigegebenen Ordnern. Sie werden automatisch mit den Originalen auf dem Dateiserver synchronisiert, sobald wieder eine Verbindung mit dem Dateiserver besteht.
- Im Synchronisierungscenter lassen sich Offlinedateien manuell synchronisieren. Das Synchronisierungscenter eignet sich auch zur Auflösung von Synchronisationskonflikten, die sich ergeben, wenn eine Offlinedatei und das freigegebene Original im selben Zeitraum geändert wurden.

- Bei der transparenten Zwischenspeicherung werden Dateien von freigegebenen Ordnern aus Remotenetzwerken automatisch zwischengespeichert. Transparent zwischengespeicherte Dateien sind nur auf dem lokalen Computer verfügbar und werden im Gegensatz zu Offlinedateien nicht synchronisiert.
- Energiesparpläne steuern die Energieverwendung von Windows 7-Computern. Standardbenutzer können ohne Anhebung der Rechte einen Energiesparplan auswählen, der ihren Anforderungen entspricht.
- Der Standardenergiesparplan von Windows 7 ist *Ausbalanciert*. Standardmäßig stehen unter Windows 7 auch noch die Pläne *Energiesparmodus* und *Höchstleistung* zur Verfügung.
- *Powercfg.exe* kann zum Export und Import von Energiesparplänen verwendet werden. Auf diese Weise lassen sich Energiesparpläne von einem Computer auf andere übertragen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 2, »Windows 7 und Mobilität«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welcher der folgenden Befehle liefert eine Liste der Geräte, die auf einem Windows 7-Computer so konfiguriert sind, dass sie den Computer aus jedem Standbymodus reaktivieren können?
   A. `Powercfg.exe -devicequery all_devices`
   B. `Powercfg.exe -hibernate on`
   C. `Powercfg.exe -devicequery wake_armed`
   D. `Powercfg.exe -list`
2. Sam Abolrous verfügt auf einem Windows 7-Client über ein Benutzerkonto, das kein Mitglied der lokalen Gruppe *Administratoren* ist. Welche der folgenden Energieeinstellungen kann Sam vornehmen? (Wählen Sie alle zutreffenden Antworten.)
   A. Auswählen eines anderen Energiesparplans
   B. Erstellen eines neuen Energiesparplans
   C. Ändern der Netzschaltereinstellungen
   D. Ändern der Einstellung *Kennwort bei Reaktivierung anfordern*

3. Mit welchem der folgenden Tools können Sie einen benutzerdefinierten Energiesparplan von einem Windows 7-Computer auf einen anderen übertragen?
   A. Seite *Energieoptionen* der Systemsteuerung
   B. *Gpedit.msc*
   C. *Powercfg.exe*
   D. *Bcdedit.exe*
4. Kim Akers hat die Datei *Brisbane.doc*, die auf einem Dateiserver des Büros liegt, offline verfügbar gemacht. Über das Wochenende arbeitet sie auf ihrem portablen Windows 7-Computer mit dieser Datei. Sam Abolrous geht am Wochenende ins Büro und arbeitet mit dem Original der Datei *Brisbane.doc*, das auf dem Dateiserver gespeichert ist. Mit welchem der folgenden Tools kann Kim den Synchronisationskonflikt auflösen, der sich ergibt, wenn sie ihren Computer wieder an das Büronetzwerk anschließt?
   A. Anmeldeinformationsverwaltung
   B. Synchronisierungscenter
   C. Heimnetzgruppe
   D. Netzwerk- und Freigabecenter
5. Welche der folgenden Richtlinien sollten Sie aktivieren, damit Windows 7-Clients Dateien von freigegebenen Ordnern zwischenspeichern können, ohne die Dateien offline verfügbar zu machen, falls die Roundtrip-Netzwerklatenz zum Remotedateiserver einen vorgegebenen Schwellenwert überschreitet?
   A. *Übertragungsrate für langsame Verbindungen konfigurieren*
   B. *Modus für langsame Verbindungen konfigurieren*
   C. *Dateien aus der Zwischenspeicherung ausschließen*
   D. *Transparentes Zwischenspeichern aktivieren*

Rückblick auf dieses Kapitel

Um den in diesem Kapitel behandelten Stoff zu vertiefen und einzuüben, können Sie folgende Aufgaben durchführen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispiel durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, Lösungen zu entwickeln.
- Arbeiten Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- BitLocker schützt Computer durch eine vollständige Verschlüsselung der Festplatte und durch den Schutz der Startumgebung vor Offlineangriffen.
- BitLocker To Go bietet für auswechselbare USB-Speichergeräte eine vollständige Verschlüsselung des Volumes. Die Daten auf den geschützten Speichergeräten sind auf anderen Computern zugänglich, wenn das entsprechende Kennwort verwendet wird.
- Offlinedateien ermöglichen auch dann die Verwendung von entsprechend konfigurierten Dateien, die in freigegebenen Ordnern liegen, auf einem Computer, wenn der Computer nicht mit dem Netzwerk verbunden ist.
- Mit dem Synchronisierungscenter können Konflikte aufgelöst werden, die sich zwischen Offlinedateien und den Originaldateien in den freigegebenen Ordnern ergeben.
- Die transparente Zwischenspeicherung ist eine Technologie zur automatischen Zwischenspeicherung, die Zugriffe auf Dateien beschleunigt, die in Remotenetzwerken auf Dateifreigaben liegen.
- Energiesparpläne ermöglichen einen Kompromiss zwischen Computerleistung und Energieverbrauch. Energiesparpläne können mit einem Befehlszeilenprogramm auf andere Computer übertragen werden.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Datenwiederherstellungsagent (DRA)**
- **Transparente Zwischenspeicherung**
- **Offlinedateien**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel können Sie Ihr Wissen zum Stoff dieses Kapitels anwenden. Die Antworten auf die Fragen finden Sie im Abschnitt »Antworten« am Ende des Buchs.

Übung 1: Zugriff auf Offlinedateien bei Contoso

Die Australien-Abteilung von Contoso besteht aus einer Zentrale in Melbourne und Zweigstellen in Wagga Wagga, Maroochydore und Wangaratta. Auf dem Dateiserver *fs1.melbourne.au.contoso.com* in Melbourne ist Windows Server 2008 installiert. Einige Benutzer in Melbourne haben Dateien auf freigegebenen Ordnern gespeichert und offline verfügbar gemacht. Gelegentlich ändern Benutzer diese Dateien, während die Benutzer, die diese Dateien offline verfügbar gemacht haben, nicht im Büro sind. Einige Clients in den Zweigstellen müssen Dateien vom Dateiserver in Melbourne herunterladen, müssen sich aber wegen einer Überlastung des WANs mit Verzögerungen abfinden. Auf den Clients in den Zweigstellen wird Windows 7 Professional verwendet. Diese Clients sind nicht Mitglieder der Domäne *Contoso*. Sie haben auf einem Client einer Zweigstelle einen benutzerdefinierten Energiesparplan eingerichtet. Sie möchten diesen Energiesparplan auch auf den anderen Windows 7-Clients der Zweigstellen verwenden.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Welches Tool können Sie verwenden, damit die anderen Clients in den Zweigstellen den gewünschten Energiesparplan erhalten?
2. Wie können Sie für die Clients in Wagga Wagga, Wangaratta und Maroochydore den Zugriff auf Dateien beschleunigen, die auf *fs1.melbourne.au.contoso.com* gespeichert sind?
3. Welches Tool sollten Sie den Benutzern in der Zentrale empfehlen, um Synchronisationskonflikte mit Offlinedateien zu lösen?

Übung 2: Verwenden von BitLocker bei Tailspin Toys

Tailspin Toys hat kürzlich eine große Zahl von Computern bereitgestellt, auf denen Windows 7 Enterprise verwendet wird. Die Firma hat außerdem USB-Flashlaufwerke mit einer Speicherkapazität von 32-GByte an die Benutzer dieser Computer ausgegeben. Da ein leitender Angestellter sein Laufwerk in der Wartehalle eines Flughafens verloren hat, werden Sie beauftragt, die Sicherheitsrichtlinien für solche Geräte zu überprüfen. Es ist wichtig, dass Unbefugte Daten von diesen Laufwerken nicht wiederherstellen können, falls eines der Geräte verloren geht. Benutzer sollen auf solchen Geräten keine Daten speichern können, solange diese Daten nicht von Tailspin Toys verschlüsselt werden. Auf ihren Heimcomputern sollen Benutzer die gespeicherten Daten aber verwenden können. Auf den Heimcomputern wird Windows XP oder Windows Vista verwendet.

Beantworten Sie vor diesem Hintergrund nun folgende Fragen:

1. Wie erreichen Sie, dass die Daten von den USB-Speichergeräten auf den Heimcomputern unter Windows XP und Windows Vista gelesen werden können?

2. Wie können Sie sicherstellen, dass Benutzer Daten nur auf Wechseldatenträgern speichern können, für die Tailspin Toys den BitLocker-Schutz eingerichtet hat?
3. Wie erreichen Sie, dass sich Daten von Wechseldatenträgern wiederherstellen lassen, wenn ein Benutzer sein Kennwort vergessen oder seinen Schlüssel verloren hat?

Vorgeschlagene Übungen

Führen Sie die folgenden Übungen durch, um den in diesem Kapitel vorgestellten prüfungsrelevanten Stoff einzuüben.

Konfigurieren von BitLocker und BitLocker To Go

Diese Übung erfordert einen Computer mit einem kompatiblen TPM-Chip. Wenn Sie nicht über einen entsprechenden Computer verfügen oder einen virtuellen Computer verwenden, überspringen Sie diese Übung.

- **Übung 1** Konfigurieren Sie einen Computer, der über einen TPM-Chip verfügt, so, dass alle angeschlossenen Volumes mit BitLocker geschützt werden. Die Verschlüsselung der Volumes kann einige Zeit erfordern.
- **Übung 2** Entfernen Sie BitLocker von dem Computer, den Sie in Übung 1 verwendet haben. Auch die Entfernung von BitLocker kann einige Zeit erfordern.

Konfigurieren der Mobilitätsoptionen

Für diese Übung brauchen Sie die beiden Computer *Canberra* und *Aberdeen*, die miteinander verbunden sein müssen. Den Computer *Aberdeen* haben Sie in Kapitel 6 konfiguriert. In dieser Übung arbeiten Sie mit Offlinedateien und versuchen, Synchronisierungsprobleme zu lösen.

- **Übung 1** Richten Sie auf dem Computer *Aberdeen* einen freigegebenen Ordner ein. Erstellen Sie mit WordPad einige Textdateien. Stellen Sie auf dem Computer *Canberra* über das Netzwerk eine Verbindung mit diesem freigegebenen Ordner her. Wenn Sie am Computer *Canberra* angemeldet sind, machen Sie auf dem Computer *Aberdeen* eine der Dateien, die Sie erstellt haben, offline verfügbar.
- **Übung 2** Nachdem Sie eine der Dateien, die Sie auf dem Computer *Aberdeen* erstellt haben, auf dem Computer *Canberra* offline verfügbar gemacht haben, fahren Sie den Computer *Aberdeen* herunter. Ändern Sie die Datei auf dem Computer *Canberra* und fahren Sie dann den Computer *Canberra* herunter. Starten Sie den Computer *Aberdeen* und ändern Sie dieselbe Datei, die Sie bereits auf dem Computer *Canberra* geändert haben. Starten Sie den Computer *Canberra*. Verwenden Sie das Synchronisierungscenter, um den Konflikt zwischen der geänderten Offlinedatei auf dem Computer *Canberra* und der geänderten freigegebenen Datei auf dem Computer *Aberdeen* zu lösen.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit allen verfügbaren Prüfungen testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« am Anfang dieses Buchs.

KAPITEL 12

Windows Update und Windows Internet Explorer

Dafür zu sorgen, dass Computer sicher sind, ist eine der wichtigsten Aufgaben eines IT-Profis. Diese Aufgabe wird zunehmend schwieriger, da auch die Angreifer dazulernen. Malwareautoren reagieren schnell auf die Veröffentlichung neuer Updates und untersuchen sie genau, um weitere Informationen über die Angriffspunkte zu erhalten, die mit den Updates beseitigt werden sollen. Das bedeutet zum Beispiel, je länger Sie die Updates nicht installieren, desto länger geben Sie Angreifern Zeit, Angriffspunkte auszunutzen, die eigentlich bereits durch Updates beseitigt worden sind. Im ersten Teil des Kapitels erfahren Sie, wie Sie Windows 7-Clients auf dem aktuellen Stand halten, um die Sicherheit der Geräte und Benutzer in Ihrer Organisation zu schützen.

Windows Internet Explorer 8 ist der Browser, der unter Windows 7 am häufigsten verwendet wird. Im Büroalltag ist das Browsen im Internet und im Intranet ebenso wichtig geworden wie die Arbeit mit einem Textverarbeitungsprogramm oder einer Tabellenkalkulation. Der zweite Teil des Kapitels beschreibt, wie Sie die beiden neuen Schutzmechanismen von Internet Explorer 8 konfigurieren: InPrivate-Browsen und InPrivate-Filterung. Sie erfahren, wie Sie den Funktionsumfang des Internet Explorers durch die Konfiguration und Verwaltung von Schnellinfos und Add-Ons erweitern. Außerdem lesen Sie, wie Sie den Internet Explorer durch die sorgfältige Konfiguration seiner Schutzmechanismen und Zoneneinstellungen sicherer machen.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren von Updates für Windows 7
- Konfigurieren von Internet Explorer

Lektionen in diesem Kapitel:

- Lektion 1: Aktualisieren von Windows 7 601
- Lektion 2: Konfigurieren von Internet Explorer 623

Bevor Sie beginnen

Zur Durchführung der Übungen dieses Kapitels sind einige Vorbereitungen erforderlich:

- Sie haben das Betriebssystem Windows 7 auf einem eigenständigen Client-PC namens *Canberra* installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.
- Sorgen Sie dafür, dass der Computer *Canberra* über eine aktive Internetverbindung verfügt.

Praxistipp

Orin Thomas

Viele Sicherheitsprobleme wären wahrscheinlich gar nicht aufgetreten, wenn Administratoren und Benutzer ihre Computer mit Softwareupdates, Antivirendefinitionen und Service Packs immer auf dem aktuellen Stand gehalten hätten. Bei einem großen Anteil der Angriffe gegen Computer werden Probleme ausgenutzt, die der Hersteller eigentlich bereits mit einem veröffentlichten Update behoben hat. Viele bekannte Viren und Würmer haben Sicherheitslücken ausgenutzt, die Microsoft bereits geschlossen hatte. Code Red, Nimda und Sasser waren zum Beispiel erfolgreich, weil eine große Zahl von Computerbenutzern ihre Computer nicht mit Softwareupdates versorgt hatten. Hätten alle Administratoren gewissenhaft Updates installiert, hätten wir vermutlich nie von diesen Viren gehört, weil sie nicht in der Lage gewesen wären, Computer zu infizieren. Die rechtzeitige Installation von Updates ist wichtig, denn Sicherheitsuntersuchungen haben zu der Schätzung geführt, dass innerhalb von einer Woche nach der Veröffentlichung eines neuen Updates bereits Code im Umlauf ist, der die vom Update beseitigten Angriffspunkte auszunutzen versucht. Einer der wichtigsten Aspekte Ihrer beruflichen Laufbahn als IT-Profi, der mit Clientcomputern zu tun hat, besteht darin, dafür zu sorgen, dass auf den von Ihnen betreuten Clients stets die neusten Softwareupdates installiert sind. Dadurch werden die von Ihnen verwalteten Computer relativ immun gegen Malwareinfektionen. Außerdem erklärt wohl niemand gerne seinem Chef oder Auftraggeber nach dem nächsten großen Viren- oder Wurmbefall, warum er nicht die Zeit gefunden hat, das Update zu installieren, das die Computer der Organisation vor dem Angriff geschützt hätte.

Lektion 1: Aktualisieren von Windows 7

Ihre Verantwortung für die Verwaltung eines Computers endet nicht, wenn das Betriebssystem und die Anwendungen installiert und konfiguriert sind und der Benutzer sich zum ersten Mal am Computer anmeldet. Als IT-Profi, der für die Verwaltung von Windows 7-Clients zuständig ist, werden Sie wahrscheinlich mehr Zeit damit verbringen, die rechtzeitige Installation von Softwareupdates und Service Packs sicherzustellen, als Sie jemals für die Installation des Betriebssystems auf neuen Computern aufwenden müssen. In dieser Lektion erfahren Sie, wie Sie die Installation von Softwareupdates automatisieren können. Sie lernen die Funktionen des Windows Update-Clients kennen, der in Windows 7 integriert ist, und wichtige Lösungen für die Bereitstellung von Updates, wie zum Beispiel WSUS (Windows Software Update Services).

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Verwalten von Updates für Windows 7
- Konfigurieren von Gruppenrichtlinien für Updates
- Konfigurieren und Aktualisieren von Updatequellen

Veranschlagte Zeit für diese Lektion: 40 Minuten

Konfigurieren von Windows Update

Die Seite *Windows Update* der Systemsteuerung ist das wichtigste Werkzeug für die Verwaltung von Softwareupdates auf Windows 7-Clients. Auf dieser Seite kann ein Benutzer, der über Administratorrechte verfügt, nach Updates suchen, Einstellungen für Updates ändern, die installierten Updates überprüfen und ausgeblendete Updates anzeigen. Ein Benutzer, der seine Rechte nicht anheben kann, kann auf dieser Seite nach Updates suchen und sie installieren. Windows Update verwendet den Dienst *Windows Update*, der auf allen Windows-Clients standardmäßig aktiviert wird.

Bei der Installation von Windows 7 werden Sie vom Installationsprogramm gefragt, wie die Standardeinstellungen für Windows Update vorgenommen werden sollen. Zur Wahl stehen die Optionen *Empfohlene Einstellungen verwenden*, *Nur wichtige Updates installieren* und *Später erneut nachfragen*. Wenn Sie die empfohlenen Einstellungen wählen, sucht Windows Update jede Nacht um 3 Uhr nach Updates, die als wichtig oder empfohlen eingestuft werden, und installiert sie. Ist der Computer um diese Zeit ausgeschaltet, sucht und installiert Windows Update die Updates nach dem nächsten Einschalten.

Administratoren und Standardbenutzer können die Suche nach Updates manuell einleiten, indem sie auf der Seite *Windows Update* auf das Element *Nach Updates suchen* klicken. Um nach Updates zu suchen, muss der Computer Kontakt zur Updatequelle herstellen können. Bei der Updatequelle kann es sich um die Microsoft Update-Server im Internet oder um lokale Updateserver handeln. Im Verlauf dieser Lektion wird noch beschrieben, wie man Windows Update so konfiguriert, dass es einen lokalen Updateserver verwendet. Sobald die Suche nach Updates beendet ist, zeigt die Seite *Windows Update* der Systemsteuerung an, wie viele Updates installiert werden können (Abbildung 12.1). Wenn Sie die Suche nach Updates manuell einleiten, statt den definierten Zeitpunkt abzuwarten, prüft Windows Update nur, ob Updates vorliegen. Bei der manuellen Überprüfung werden Updates nicht auto-

matisch heruntergeladen und installiert. Mit folgendem Befehl können Sie die Suche nach Updates auch auf der Befehlszeile einleiten:

```
Wuauclt.exe /detectnow
```


« System und Sicherheit ▸ Windows Update
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Nach Updates suchen
Einstellungen ändern
Updateverlauf anzeigen
Ausgeblendete Updates anzeigen
Updates: Häufig gestellte Fragen (FAQ)
Windows Update
Updates für den Computer herunterladen und installieren
9 wichtige Updates sind verfügbar
36 optionale Updates sind verfügbar
9 wichtige Updates ausgewählt, 29,9 MB
Updates installieren
Updates wurden zuletzt gesucht: Heute um 15:04
Updates wurden installiert: Nie
Sie erhalten Updates: Nur für Windows
Rufen Sie Updates für weitere Microsoft-Produkte ab. Weitere Informationen
Siehe auch
Installierte Updates

Abbildung 12.1 Die Seite *Windows Update* der Systemsteuerung

Updates werden in drei Gruppen aufgeteilt:

- **Wichtige Updates** Wichtige Updates beheben häufig kritische Sicherheitsprobleme. In manchen Fällen sind Updates mit dieser Klassifikation dafür vorgesehen, Sicherheitslücken zu schließen, die von Angreifern aus dem Internet bereits ausgenutzt werden.

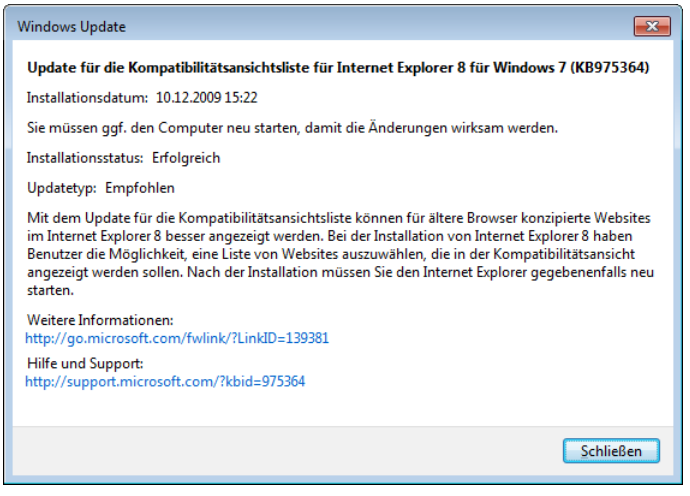

Windows Update
Update für die Kompatibilitätsansichtsliste für Internet Explorer 8 für Windows 7 (KB975364)
Installationsdatum: 10.12.2009 15:22
Sie müssen ggf. den Computer neu starten, damit die Änderungen wirksam werden.
Installationsstatus: Erfolgreich
Updatetyp: Empfohlen
Mit dem Update für die Kompatibilitätsansichtsliste können für ältere Browser konzipierte Websites im Internet Explorer 8 besser angezeigt werden. Bei der Installation von Internet Explorer 8 haben Benutzer die Möglichkeit, eine Liste von Websites auszuwählen, die in der Kompatibilitätsansicht angezeigt werden sollen. Nach der Installation müssen Sie den Internet Explorer gegebenenfalls neu starten.
Weitere Informationen:
http://go.microsoft.com/fwlink/?LinkID=139381
Hilfe und Support:
http://support.microsoft.com/?kbid=975364
Schließen

Abbildung 12.2 Eigenschaften eines empfohlenen Updates

- **Empfohlene Updates** Empfohlene Updates beheben oft Funktionsprobleme. Das empfohlene Update aus Abbildung 12.2 verbessert zum Beispiel die Darstellung von Websites, die für ältere Browser konzipiert sind.
- **Optionale Updates** Optionale Updates bieten zum Beispiel Treiberupdates und Sprachpakete. Abbildung 12.3 zeigt das russische Sprachpaket, das als optionales Update für Windows 7 verfügbar ist.

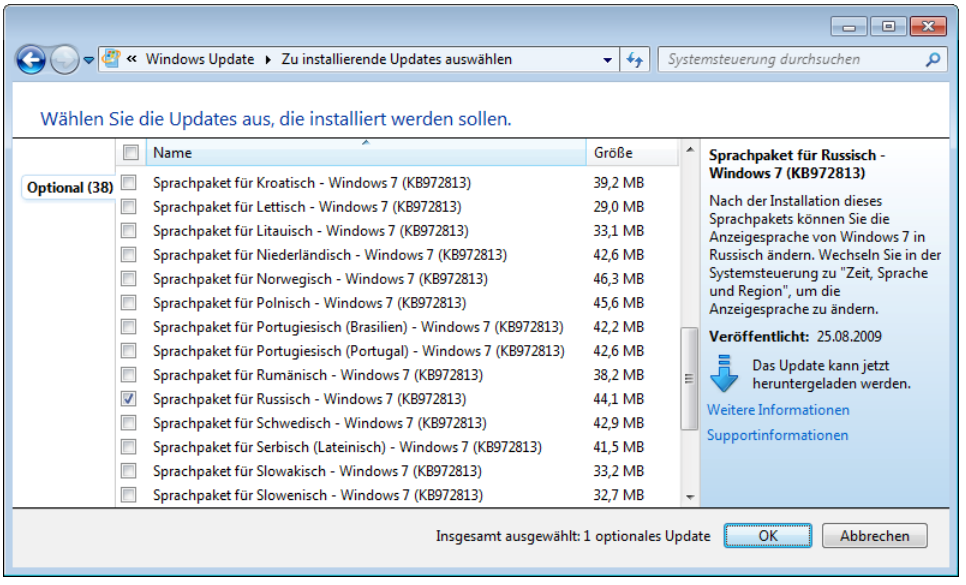

« Windows Update ▸ Zu installierende Updates auswählen
Systemsteuerung durchsuchen
Wählen Sie die Updates aus, die installiert werden sollen.
Optional (38)
Name
Größe
Sprachpaket für Kroatisch - Windows 7 (KB972813) 39,2 MB
Sprachpaket für Lettisch - Windows 7 (KB972813) 29,0 MB
Sprachpaket für Litauisch - Windows 7 (KB972813) 33,1 MB
Sprachpaket für Niederländisch - Windows 7 (KB972813) 42,6 MB
Sprachpaket für Norwegisch - Windows 7 (KB972813) 46,3 MB
Sprachpaket für Polnisch - Windows 7 (KB972813) 45,6 MB
Sprachpaket für Portugiesisch (Brasilien) - Windows 7 (KB972813) 42,2 MB
Sprachpaket für Portugiesisch (Portugal) - Windows 7 (KB972813) 42,6 MB
Sprachpaket für Rumänisch - Windows 7 (KB972813) 38,2 MB
Sprachpaket für Russisch - Windows 7 (KB972813) 44,1 MB
Sprachpaket für Schwedisch - Windows 7 (KB972813) 42,9 MB
Sprachpaket für Serbisch (Lateinisch) - Windows 7 (KB972813) 41,5 MB
Sprachpaket für Slowakisch - Windows 7 (KB972813) 33,2 MB
Sprachpaket für Slowenisch - Windows 7 (KB972813) 32,7 MB
Sprachpaket für Russisch - Windows 7 (KB972813)
Nach der Installation dieses Sprachpakets können Sie die Anzeigesprache von Windows 7 in Russisch ändern. Wechseln Sie in der Systemsteuerung zu "Zeit, Sprache und Region", um die Anzeigesprache zu ändern.
Veröffentlicht: 25.08.2009
Das Update kann jetzt heruntergeladen werden.
Weitere Informationen
Supportinformationen
Insgesamt ausgewählt: 1 optionales Update
OK
Abbrechen

Abbildung 12.3 Optionale Sprachpakete

Wie Windows Update mit Updates umgeht, hängt davon ab, welche Einstellungen Sie vorgenommen haben. Um die Einstellungen manuell zu ändern, klicken Sie auf das Element *Einstellungen ändern*. Dadurch öffnet sich die Seite *Einstellungen ändern* (Abbildung 12.4).

Auf dieser Seite können Sie festlegen, wie Windows 7 mit wichtigen Updates umgeht, wie oft eine Überprüfung auf neue Updates erfolgt, ob empfohlene Updates in der gleichen Weise wie wichtige Updates behandelt werden und ob Benutzer ohne Administratorrechte auf dem Computer Updates installieren können. Nur Benutzer mit Administratorrechten können die Einstellungen für Windows Update ändern. Auf dieser Seite können Sie folgende Einstellungen vornehmen:

- **Updates automatisch installieren (empfohlen)** Windows Update installiert Updates zur angegebenen Zeit automatisch. Das ist die Standardeinstellung von Windows Update.
- **Updates herunterladen, aber Installation manuell durchführen** Updates werden auf den Computer heruntergeladen und der Benutzer wird darüber informiert, dass Updates zur Installation bereitstehen.
- **Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen** Der Benutzer wird darüber informiert, dass neue Updates heruntergeladen und installiert werden können.

- **Nie nach Updates suchen (nicht empfohlen)** Windows Update sucht nicht automatisch nach Updates, aber die Prüfung und Installation kann manuell erfolgen.
- **Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen** Das bedeutet, dass empfohlene Updates in der gleichen Weise wie wichtige Updates behandelt werden. Optionale Updates müssen dagegen manuell installiert werden.
- **Allen Benutzern das Installieren von Updates auf diesem Computer ermöglichen** Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie es deaktivieren, können nur Mitglieder der lokalen Gruppe *Administratoren* Updates installieren.

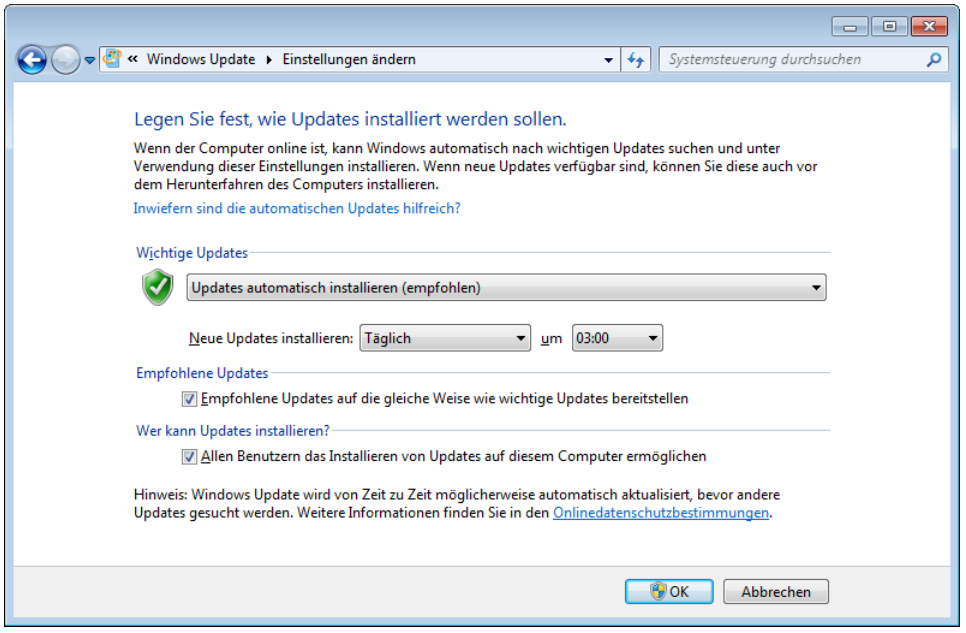

« Windows Update ▸ Einstellungen ändern
Systemsteuerung durchsuchen
Legen Sie fest, wie Updates installiert werden sollen.
Wenn der Computer online ist, kann Windows automatisch nach wichtigen Updates suchen und unter Verwendung dieser Einstellungen installieren. Wenn neue Updates verfügbar sind, können Sie diese auch vor dem Herunterfahren des Computers installieren.
Inwiefern sind die automatischen Updates hilfreich?
Wichtige Updates
Updates automatisch installieren (empfohlen)
Neue Updates installieren: Täglich um 03:00
Empfohlene Updates
Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen
Wer kann Updates installieren?
Allen Benutzern das Installieren von Updates auf diesem Computer ermöglichen
Hinweis: Windows Update wird von Zeit zu Zeit möglicherweise automatisch aktualisiert, bevor andere Updates gesucht werden. Weitere Informationen finden Sie in den Onlinedatenschutzbestimmungen.
OK
Abbrechen

Abbildung 12.4 Wie Windows Updates installiert, lässt sich einstellen

Die Seite *Updateverlauf anzeigen* zeigt eine Liste aller Updates, die mit oder ohne Erfolg auf dem Computer installiert wurden, sowie das Installationsdatum und die Klassifikation (Abbildung 12.5). Wenn Sie auf der Seite *Updateverlauf anzeigen* ein Update doppelt anklicken, erhalten Sie weitere Informationen darüber. Dazu gehört eine kurze Beschreibung des Updates und eine Verknüpfung zu einem KnowledgeBase-Artikel, in dem das Update ausführlicher beschrieben wird. In den KnowledgeBase-Artikeln wird auch beschrieben, welche Probleme ein Update möglicherweise verursachen kann. Wenn Sie auf einem Windows 7-Client ein Update installieren und sich unerwartete Probleme zeigen, sollten Sie den betreffenden KnowledgeBase-Artikel für das Update lesen und überprüfen, ob die Probleme bereits dokumentiert sind und ob Lösungen beschrieben werden. Wenn Sie ein Update löschen möchten, sollten Sie die KnowledgeBase-Kennung des Updates kennen. Die KnowledgeBase-Kennung ist eine 6-stellige Zahl, vor der meistens die Buchstaben KB stehen, wie zum Beispiel in KB123456.

Wenn Sie Updates überprüfen, die zur Installation bereitstehen, können Sie ein Update auch mit der rechten Maustaste anklicken und *Update ausblenden* wählen. Dann wird das Update praktisch nicht mehr mitgezählt. Anders gesagt, es wird nicht installiert und Windows Update bietet das spezielle Update zukünftig nicht mehr zur Installation über Windows Update an.

Nur Benutzer mit Administratorrechten können Updates ausblenden. Ein Update auszublenden bedeutet nicht, dass es später nicht mehr installiert werden kann. Mit dem Element *Ausgeblendete Updates anzeigen* auf der Seite *Windows Update* der Systemsteuerung können Sie alle bereits ausgeblendeten Updates anzeigen und bei Bedarf wieder einblenden. Sie werden dann wieder mitgezählt und sind bei der nächsten Überprüfung auf Updates wieder verfügbar. Abbildung 12.6 zeigt die Seite *Ausgeblendete Updates anzeigen*.

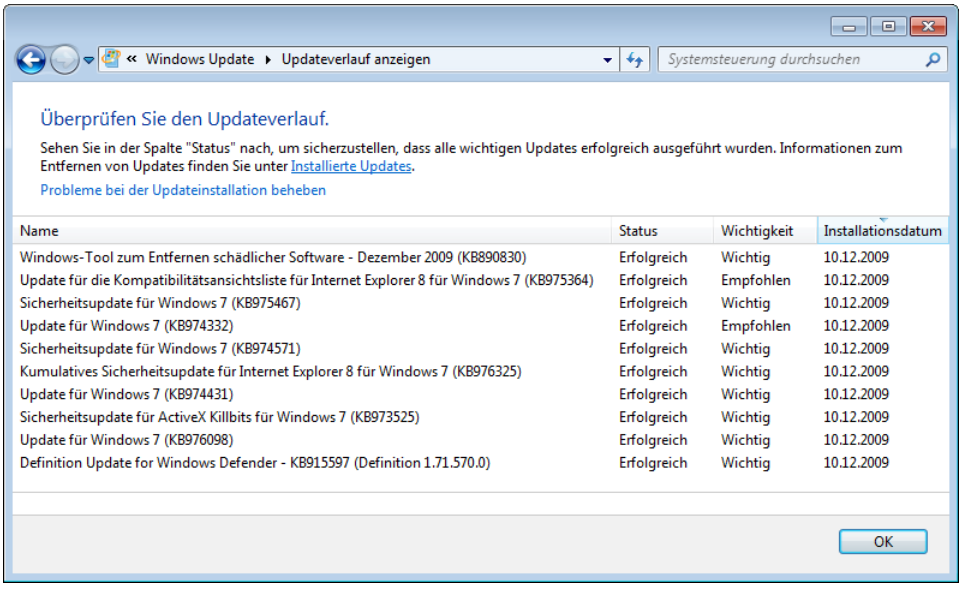

« Windows Update ▸ Updateverlauf anzeigen
Systemsteuerung durchsuchen
Überprüfen Sie den Updateverlauf.
Sehen Sie in der Spalte "Status" nach, um sicherzustellen, dass alle wichtigen Updates erfolgreich ausgeführt wurden. Informationen zum Entfernen von Updates finden Sie unter Installierte Updates.
Probleme bei der Updateinstallation beheben
Name
Status
Wichtigkeit
Installationsdatum
Windows-Tool zum Entfernen schädlicher Software - Dezember 2009 (KB890830) Erfolgreich Wichtig 10.12.2009
Update für die Kompatibilitätsansichtsliste für Internet Explorer 8 für Windows 7 (KB975364) Erfolgreich Empfohlen 10.12.2009
Sicherheitsupdate für Windows 7 (KB975467) Erfolgreich Wichtig 10.12.2009
Update für Windows 7 (KB974332) Erfolgreich Empfohlen 10.12.2009
Sicherheitsupdate für Windows 7 (KB974571) Erfolgreich Wichtig 10.12.2009
Kumulatives Sicherheitsupdate für Internet Explorer 8 für Windows 7 (KB976325) Erfolgreich Wichtig 10.12.2009
Update für Windows 7 (KB974431) Erfolgreich Wichtig 10.12.2009
Sicherheitsupdate für ActiveX Killbits für Windows 7 (KB973525) Erfolgreich Wichtig 10.12.2009
Update für Windows 7 (KB976098) Erfolgreich Wichtig 10.12.2009
Definition Update for Windows Defender - KB915597 (Definition 1.71.570.0) Erfolgreich Wichtig 10.12.2009
OK

Abbildung 12.5 Anzeigen des Updateverlaufs

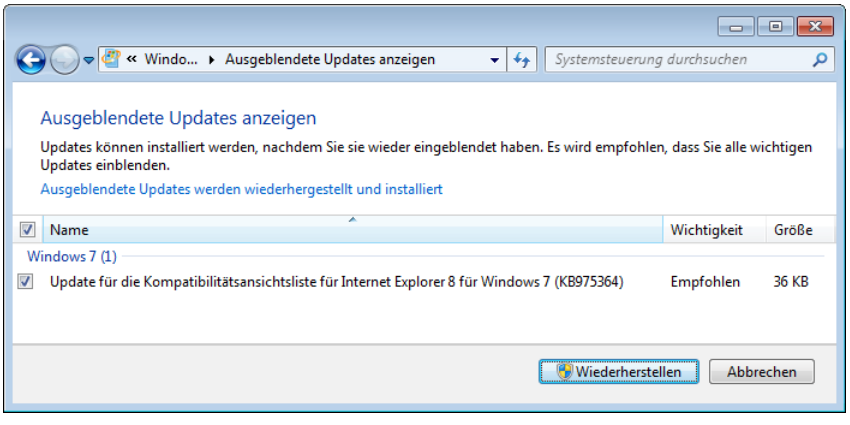

« Windo... ▸ Ausgeblendete Updates anzeigen
Systemsteuerung durchsuchen
Ausgeblendete Updates anzeigen
Updates können installiert werden, nachdem Sie sie wieder eingeblendet haben. Es wird empfohlen, dass Sie alle wichtigen Updates einblenden.
Ausgeblendete Updates werden wiederhergestellt und installiert
Name
Wichtigkeit
Größe
Windows 7 (1)
Update für die Kompatibilitätsansichtsliste für Internet Explorer 8 für Windows 7 (KB975364) Empfohlen 36 KB
Wiederherstellen
Abbrechen

Abbildung 12.6 Anzeigen ausgeblendeter Updates

Es ist möglich, ein bereits installiertes Update wieder zu deinstallieren. Ein Benutzer, der Mitglied der lokalen Gruppe *Administratoren* ist, kann ein Update deinstallieren. Die Deinstallation erfolgt auf der Seite *Programme und Funktionen* der Systemsteuerung. Diese Seite erreichen Sie zum Beispiel, wenn Sie auf der Seite *Windows Update* der Systemsteuerung auf das Element *Installierte Updates* klicken. Im Gegensatz zur Seite *Updateverlauf*

anzeigen werden außer einer kurzen allgemeinen Bezeichnung nur die KnowledgeBase-Kennungen der Updates angezeigt. Das bedeutet, dass Sie die KnowledgeBase-Kennung eines Updates kennen müssen, um es zu deinstallieren. Wie bereits beschrieben, können Sie die KnowledgeBase-Kennung eines bestimmten Updates ermitteln, wenn Sie das Update auf der Seite *Updateverlauf anzeigen* heraussuchen und doppelt anklicken. Dadurch öffnet sich ein Dialogfeld mit Informationen über das Update, in dem Sie die KnowledgeBase-Kennung ermitteln können (Abbildung 12.7).


Windows Update
Update für die Kompatibilitätsansichtsliste für Internet Explorer 8 für Windows 7 (KB975364)
Installationsdatum: 10.12.2009 15:22
Sie müssen ggf. den Computer neu starten, damit die Änderungen wirksam werden.
Installationsstatus: Erfolgreich
Updatetyp: Empfohlen
Mit dem Update für die Kompatibilitätsansichtsliste können für ältere Browser konzipierte Websites im Internet Explorer 8 besser angezeigt werden. Bei der Installation von Internet Explorer 8 haben Benutzer die Möglichkeit, eine Liste von Websites auszuwählen, die in der Kompatibilitätsansicht angezeigt werden sollen. Nach der Installation müssen Sie den Internet Explorer gegebenenfalls neu starten.
Weitere Informationen:
http://go.microsoft.com/fwlink/?LinkID=139381
Hilfe und Support:
http://support.microsoft.com/?kbid=975364
Schließen

Abbildung 12.7 Informationen über ein Update

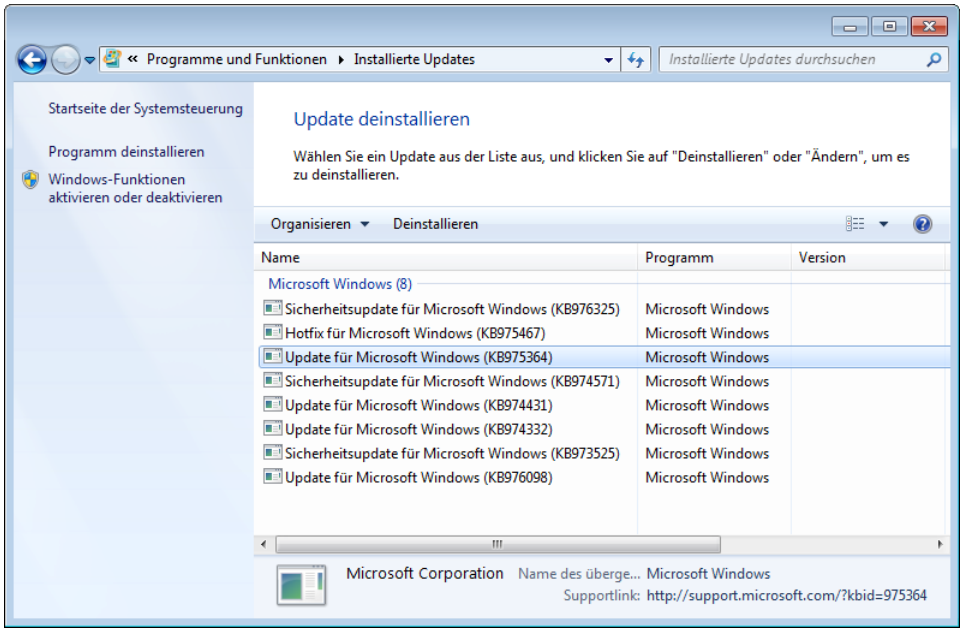

« Programme und Funktionen ▸ Installierte Updates
Installierte Updates durchsuchen
Startseite der Systemsteuerung
Programm deinstallieren
Windows-Funktionen aktivieren oder deaktivieren
Update deinstallieren
Wählen Sie ein Update aus der Liste aus, und klicken Sie auf "Deinstallieren" oder "Ändern", um es zu deinstallieren.
Organisieren
Deinstallieren
Name
Programm
Version
Microsoft Windows (8)
Sicherheitsupdate für Microsoft Windows (KB976325) Microsoft Windows
Hotfix für Microsoft Windows (KB975467) Microsoft Windows
Update für Microsoft Windows (KB975364) Microsoft Windows
Sicherheitsupdate für Microsoft Windows (KB974571) Microsoft Windows
Update für Microsoft Windows (KB974431) Microsoft Windows
Update für Microsoft Windows (KB974332) Microsoft Windows
Sicherheitsupdate für Microsoft Windows (KB973525) Microsoft Windows
Update für Microsoft Windows (KB976098) Microsoft Windows
Microsoft Corporation
Name des überge... Microsoft Windows
Supportlink: http://support.microsoft.com/?kbid=975364

Abbildung 12.8 Deinstallieren eines Updates

Wenn Sie ein Update deinstallieren, erscheint es nicht automatisch in der Liste der ausgeblendeten Updates, sondern wird bei der nächsten Prüfung auf neue Updates wieder zur Installation verfügbar. Daher ist es wichtig, Updates nach der Deinstallation auszublenden. Wenn Sie beispielsweise feststellen, dass sich nach der Installation eines bestimmten Updates Konflikte mit einer Anwendung ergeben, die in Ihrer Organisation verwendet wird, können Sie das Update deinstallieren, damit sich die Anwendung wieder verwenden lässt. Anschließend blenden Sie das Update aus, bis der Hersteller der Software die Kompatibilitätsprobleme mit dem Update behoben hat. Dadurch ist sichergestellt, dass andere Benutzer, die Updates installieren dürfen, dieses eine Update nicht installieren können, bis das Kompatibilitätsproblem behoben ist. Abbildung 12.8 zeigt die Seite *Installierte Updates*, auf der Sie ein Update deinstallieren können.

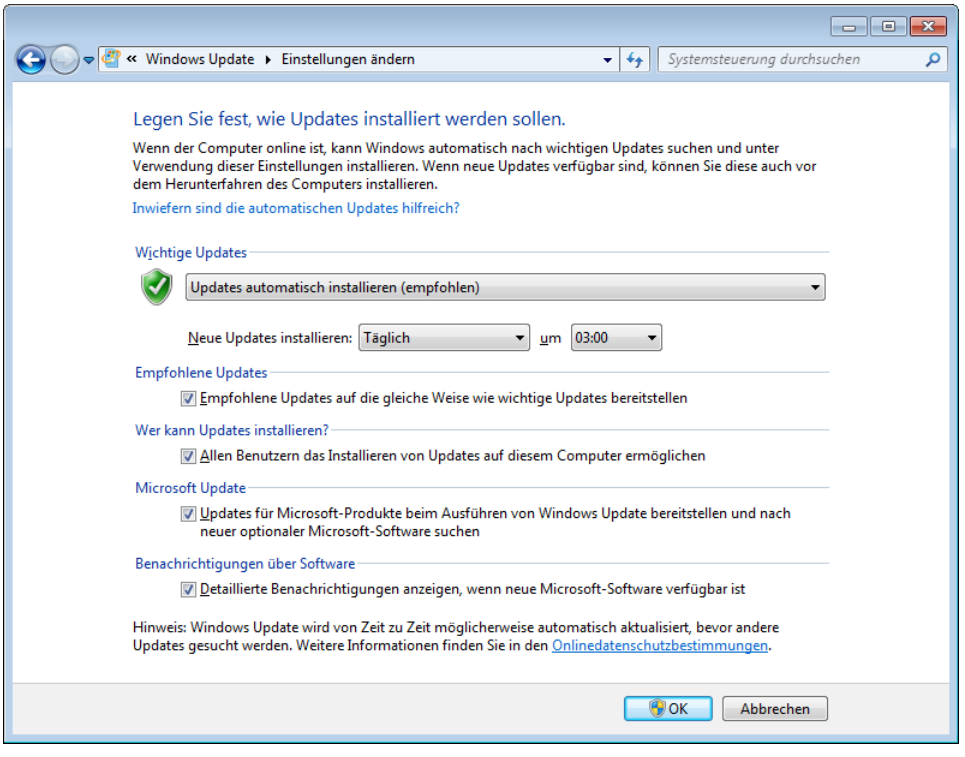

« Windows Update ▸ Einstellungen ändern
Systemsteuerung durchsuchen
Legen Sie fest, wie Updates installiert werden sollen.
Wenn der Computer online ist, kann Windows automatisch nach wichtigen Updates suchen und unter Verwendung dieser Einstellungen installieren. Wenn neue Updates verfügbar sind, können Sie diese auch vor dem Herunterfahren des Computers installieren.
Inwiefern sind die automatischen Updates hilfreich?
Wichtige Updates
Updates automatisch installieren (empfohlen)
Neue Updates installieren: Täglich um 03:00
Empfohlene Updates
Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen
Wer kann Updates installieren?
Allen Benutzern das Installieren von Updates auf diesem Computer ermöglichen
Microsoft Update
Updates für Microsoft-Produkte beim Ausführen von Windows Update bereitstellen und nach neuer optionaler Microsoft-Software suchen
Benachrichtigungen über Software
Detaillierte Benachrichtigungen anzeigen, wenn neue Microsoft-Software verfügbar ist
Hinweis: Windows Update wird von Zeit zu Zeit möglicherweise automatisch aktualisiert, bevor andere Updates gesucht werden. Weitere Informationen finden Sie in den Onlinedatenschutzbestimmungen.
OK
Abbrechen

Abbildung 12.9 Updates für andere Microsoft-Produkte

Updates für andere Microsoft-Produkte

Mit den Standardeinstellungen ruft Windows Update nur Updates für das Betriebssystem Windows und darin enthaltene Anwendungen ab. Sie können Windows Update aber aktualisieren, damit auch Updates für andere Microsoft-Produkte erkannt und mit Windows Update installiert werden können, beispielsweise Updates für Microsoft Office. Dazu klicken Sie auf der Seite *Windows Update* neben dem Text *Rufen Sie Updates für weitere Microsoft-Produkte ab* auf das Element *Weitere Informationen*. Es öffnet sich eine Webseite, die Ihnen ein Update anbietet, mit dem Sie die Funktionen von Windows Update erweitern können. Durch die Installation dieses Updates wird ein Abschnitt zur Seite *Einstellungen ändern* hinzugefügt, mit dem Sie Windows Update anweisen können, auch für andere Microsoft-

Produkte Updates anzufordern (Abbildung 12.9). Außerdem kann Windows Update auch Updates aus anderen Updatequellen installieren, beispielsweise von einem WSUS-Server. WSUS wird weiter unten im Kapitel ausführlicher beschrieben.

Konfigurieren von Windows Update mit einem Proxyserver

In Netzwerken mit speziellen Firewall- und Proxykonfigurationen kann es passieren, dass Windows Update-Clients keine Verbindung mit den Microsoft Update-Servern aus dem Internet herstellen können. Für dieses Problem gibt es verschiedene Lösungen. Die erste ist, im lokalen Netzwerk einen WSUS-Server bereitzustellen und die Clients so zu konfigurieren, dass sie Updates von diesem WSUS-Server herunterladen. Den WSUS-Server können Sie so konfigurieren, dass er einen Proxy verwendet. Als Alternative wäre es möglich, einen Windows 7-Client manuell so zu konfigurieren, dass Windows Update über den Proxy mit den Microsoft Update-Servern kommunizieren kann. Sie können den Internet Explorer zwar in den Internetoptionen so konfigurieren, dass er einen Proxy verwenden kann, aber Windows Update kann diese Einstellungen nicht direkt verwenden. Windows 7-Clients können Proxyeinstellungen auf zwei Arten bestimmen:

- **Verwenden von Web Proxy Auto Detect (WPAD)** Diese Funktion ermöglicht es Computern, einen verfügbaren Proxy durch die Abfrage einer DHCP-Option (Dynamic Host Configuration Protocol) oder durch einen DNS-Datensatz (Domain Name System) zu finden.
- **Verwenden des Befehlszeilentools *Netsh.exe*** Windows Update verwendet die Internetoptionen zwar nicht direkt, aber Sie können das Befehlszeilentool *Netsh.exe* verwenden, um die Proxyeinstellungen zu importieren, die für den Internet Explorer festgelegt wurden. Dazu verwenden Sie in einer Eingabeaufforderung mit erhöhten Rechten folgenden Befehl:

  ```
  netsh winhttp import proxy source=ie
  ```



Weitere Informationen Web Proxy Auto Detect

Weitere Informationen über die Konfiguration von Web Proxy Auto Detect auf DNS- und DHCP-Servern finden Sie in dem folgenden Dokument im Microsoft TechNet: *http://technet.microsoft.com/en-us/library/cc713344.aspx*.

Manuelles Installieren von Windows 7-Updatedateien

In manchen Fällen ist es erforderlich, Updatedateien manuell zu installieren, beispielsweise auf eigenständigen Computern, die nicht mit einem Netzwerk verbunden sind. Sie können die Windows 7-Updatedateien direkt von der Microsoft-Website herunterladen. Welche Updates veröffentlicht wurden, erfahren Sie zum Beispiel durch die Suche nach Updates auf einem Computer, auf dem sich Windows Update einsetzen lässt. Updatedateien haben die Dateinamenserweiterung *.msu*. Wenn Sie mehrere MSU-Dateien installieren möchten, können Sie ein entsprechendes Skript schreiben, in dem Sie das Hilfsprogramm *Wusa.exe* verwenden. Unterdrücken Sie bei jeder Updateinstallation bis auf die letzte den Neustart des Computers mit der Option `/norestart`. Das folgende Skript installiert z.B. drei Updates:

```
Wusa.exe d:\Windows6.1-kb123456-x64.msu /quiet /norestart
Wusa.exe d:\Windows6.1-kb123457-x64.msu /quiet /norestart
Wusa.exe d:\Windows6.1-kb123458-x64.msu /quiet
```

Weitere Informationen Eigenständiges Windows Update-Installationsprogramm

Weitere Informationen über das eigenständige Windows Update-Installationsprogramm (*Wusa.exe*) finden Sie in folgendem Artikel: *http://support.microsoft.com/kb/934307*.

Schnelltest

- Welche Aufgaben kann ein Standardbenutzer in Windows Update durchführen?

Antwort zum Schnelltest

- Ein Standardbenutzer kann Updates installieren. Ein Standardbenutzer kann keine Updates deinstallieren und die Updateeinstellungen nicht ändern.

Wartungscenter

Das Wartungscenter ist ein zentraler Ort für die Anzeige von Problemen aus den Bereichen Sicherheit und Wartung (Abbildung 12.10).

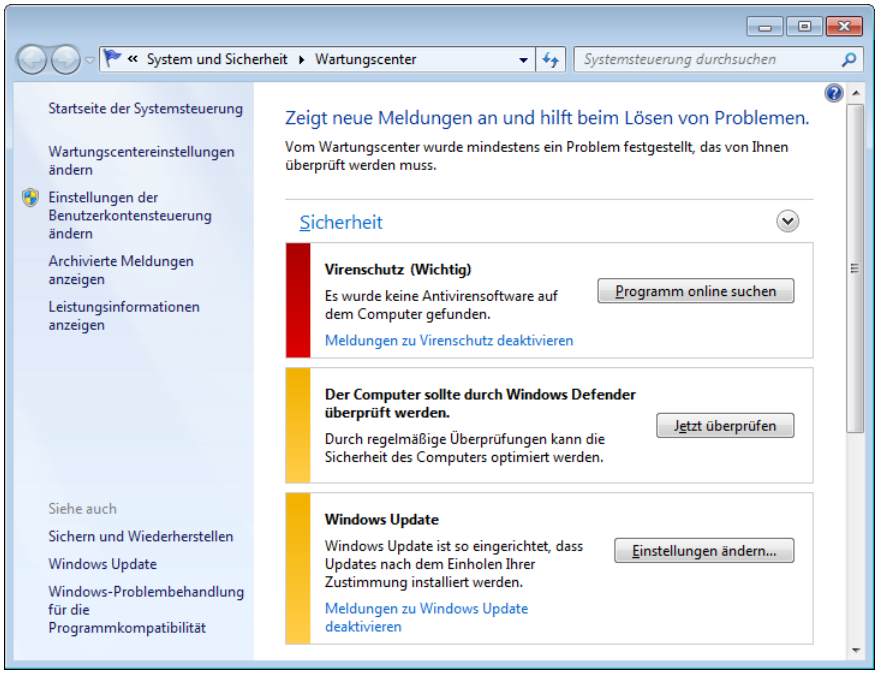

« System und Sicherheit ▸ Wartungscenter
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Wartungscentereinstellungen ändern
Einstellungen der Benutzerkontensteuerung ändern
Archivierte Meldungen anzeigen
Leistungsinformationen anzeigen
Zeigt neue Meldungen an und hilft beim Lösen von Problemen.
Vom Wartungscenter wurde mindestens ein Problem festgestellt, das von Ihnen überprüft werden muss.
Sicherheit
Virenschutz (Wichtig)
Es wurde keine Antivirensoftware auf dem Computer gefunden.
Programm online suchen
Meldungen zu Virenschutz deaktivieren
Der Computer sollte durch Windows Defender überprüft werden.
Durch regelmäßige Überprüfungen kann die Sicherheit des Computers optimiert werden.
Jetzt überprüfen
Windows Update
Windows Update ist so eingerichtet, dass Updates nach dem Einholen Ihrer Zustimmung installiert werden.
Einstellungen ändern...
Meldungen zu Windows Update deaktivieren
Siehe auch
Sichern und Wiederherstellen
Windows Update
Windows-Problembehandlung für die Programmkompatibilität

Abbildung 12.10 Wartungscenter

Meldungen des Wartungscenters erscheinen als Sprechblasen auf der Taskleiste, mit denen Benutzer daran erinnert werden, sich um bestimmte Probleme zu kümmern, die auf ihrem Computer bestehen. Das Wartungscenter kann Meldungen aus den Bereichen Sicherheit und Wartung für folgende Komponenten anzeigen:

- Windows Update
- Internet-Sicherheitseinstellungen

- Firewall
- Schutz vor Spyware und ähnliche Schutzmaßnahmen
- Benutzerkontensteuerung (UAC)
- Virenschutz
- Windows-Sicherung
- Windows-Problembehandlung

Das Wartungscenter ist auf den Dienst *Sicherheitscenter* angewiesen. Wenn der Dienst nicht aktiv ist, funktioniert das Wartungscenter nicht. Auch andere Netzwerkdienste sind auf den Dienst *Sicherheitscenter* angewiesen, beispielsweise der Netzwerkzugriffsschutz, der verhindert, dass Computer, die nicht die Integritätsanforderungen erfüllen, eine Verbindung mit dem lokalen Netzwerk oder einem virtuellen Netzwerk herstellen. Ein Benutzer mit Administratorrechten kann das Wartungscenter konfigurieren und festlegen, welche Arten von Meldungen angezeigt werden sollen (Abbildung 12.11). Sie erreichen dieses Dialogfeld, indem Sie auf der Seite *Wartungscenter* der Systemsteuerung auf das Element *Wartungscentereinstellungen ändern* klicken. Das Wartungscenter wird in Kapitel 13, »Überwachung und Leistung«, ausführlicher beschrieben.

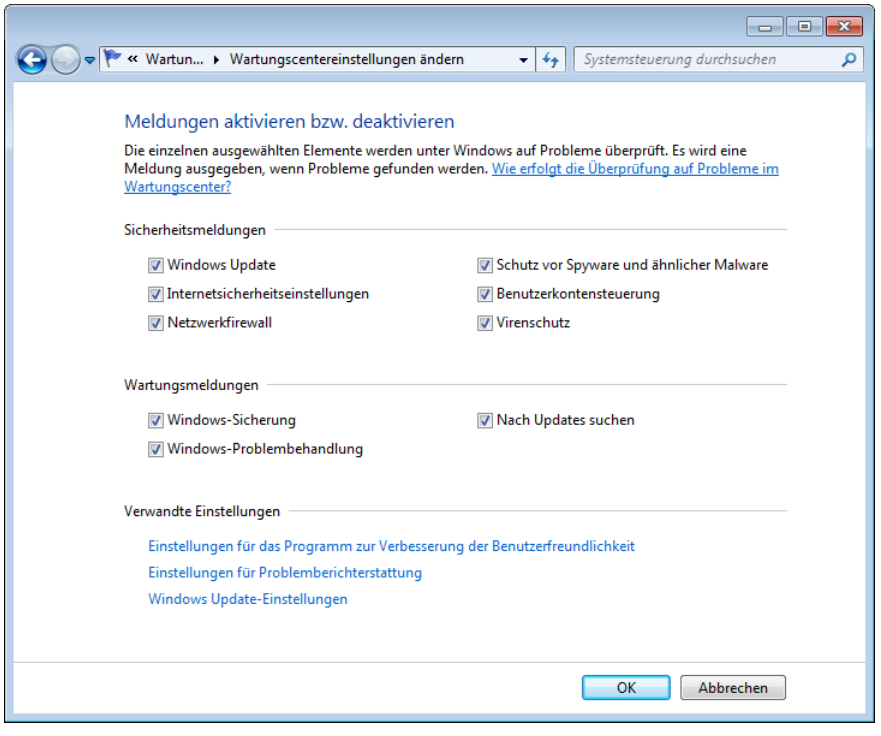


Abbildung 12.11 Einstellungen des Wartungscenters

Windows Server Update Services

Windows Update ruft Updates von den Microsoft Update-Servern aus dem Internet ab. In kleinen Umgebungen funktioniert das sehr gut, aber wenn im selben Netzwerk 10 oder mehr Computer vorhanden sind, auf denen Windows 7 verwendet wird, können Sie die Netzwerk-

belastung durch eine zentrale Softwareupdatelösung wie Windows Server Update Services (WSUS), System Center Essentials oder System Center Configuration Manager 2007 (SCCM 2007) deutlich verringern. Diese Produkte funktionieren wie ein lokaler Microsoft Update-Server. Die Clients laden nicht mehr jedes einzelne Update nur für sich über die Internetverbindung der Organisation herunter, sondern fordern es vom lokalen Updateserver an. Der Updateserver wiederum braucht jedes Update nur ein einziges Mal über die Internetverbindung herunterzuladen. Da Updatebereitstellungen mit den System Center Essentials und SCCM auf WSUS aufbauen, beschränken wir uns an dieser Stelle auf WSUS. Für Windows 7-Clients ist es erforderlich, dass auf dem WSUS-Server WSUS 3.0 mit Service Pack 1 oder höher verwendet wird.



Weitere Informationen SCCM 2007

Weitere Informationen über SCCM 2007 finden Sie auf folgender Website: *http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx*.

WSUS ermöglicht es Administratoren, Updates nach einem Zeitplan bereitzustellen, der sich am besten für die Organisation eignet. Windows Update hat den Nachteil, dass Updates nach dem Zeitplan von Microsoft veröffentlicht werden. Wenn Windows Update so eingestellt ist, dass alle neuen Updates installiert werden, hat eine Organisation nicht die Gelegenheit zu überprüfen, ob ein Update zu den Clientcomputern kompatibel ist. Wenn eine Organisation WSUS verwendet, kann sie ein Update auf einer kleinen Gruppe von Computern testen, bevor es auf allen Computern der Organisation installiert wird. Abbildung 12.12 zeigt die WSUS-Konsole auf einem Windows Server 2008-Computer.

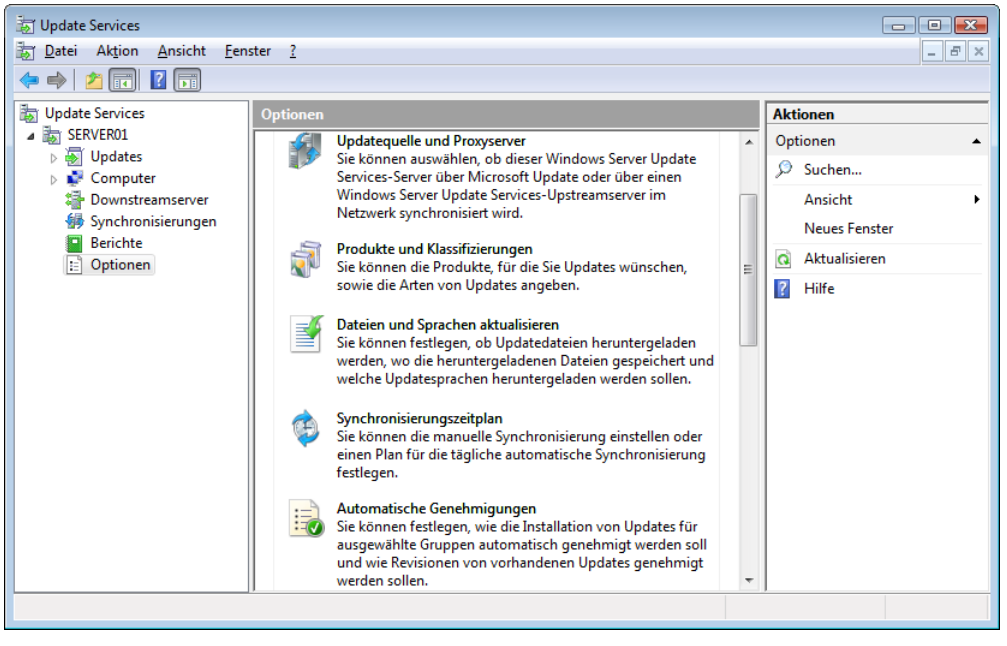

Update Services
Datei Aktion Ansicht Fenster ?
Update Services
SERVER01
Updates
Computer
Downstreamserver
Synchronisierungen
Berichte
Optionen
Optionen
Updatequelle und Proxyserver
Sie können auswählen, ob dieser Windows Server Update Services-Server über Microsoft Update oder über einen Windows Server Update Services-Upstreamserver im Netzwerk synchronisiert wird.
Produkte und Klassifizierungen
Sie können die Produkte, für die Sie Updates wünschen, sowie die Arten von Updates angeben.
Dateien und Sprachen aktualisieren
Sie können festlegen, ob Updatedateien heruntergeladen werden, wo die heruntergeladenen Dateien gespeichert und welche Updatesprachen heruntergeladen werden sollen.
Synchronisierungszeitplan
Sie können die manuelle Synchronisierung einstellen oder einen Plan für die tägliche automatische Synchronisierung festlegen.
Automatische Genehmigungen
Sie können festlegen, wie die Installation von Updates für ausgewählte Gruppen automatisch genehmigt werden soll und wie Revisionen von vorhandenen Updates genehmigt werden sollen.
Aktionen
Optionen
Suchen...
Ansicht
Neues Fenster
Aktualisieren
Hilfe

Abbildung 12.12 Die WSUS-Konsole

In vielen WSUS-Bereitstellungen kontrolliert ein Administrator Updates zentral. Das bedeutet, dass die Entscheidung, welche Updates installiert werden sollen und wann die Installation erfolgen soll, zentral erfolgt und nicht auf jedem einzelnen Clientcomputer. Die getroffenen Entscheidungen können mithilfe von Updaterichtlinien umgesetzt werden. Die Konfiguration der Updaterichtlinien wird im Verlauf der Lektion ausführlicher beschrieben.

WSUS ermöglicht es, die vorhandenen Clientcomputer in Gruppen aufzuteilen. Gruppen wiederum machen es möglich, Updates stufenweise bereitzustellen oder selektiv nur auf bestimmten Computern zu installieren. Gruppen werden auf dem WSUS-Server eingerichtet. Nach der Definition der Gruppen auf dem WSUS-Server können Sie die Clients mit der Richtlinie *Clientseitige Zielzuordnung aktivieren*, die später noch beschrieben wird, der gewünschte Zielgruppe zuordnen, oder Sie nehmen die Gruppenzuordnung in der WSUS-Konsole manuell vor (Abbildung 12.13).

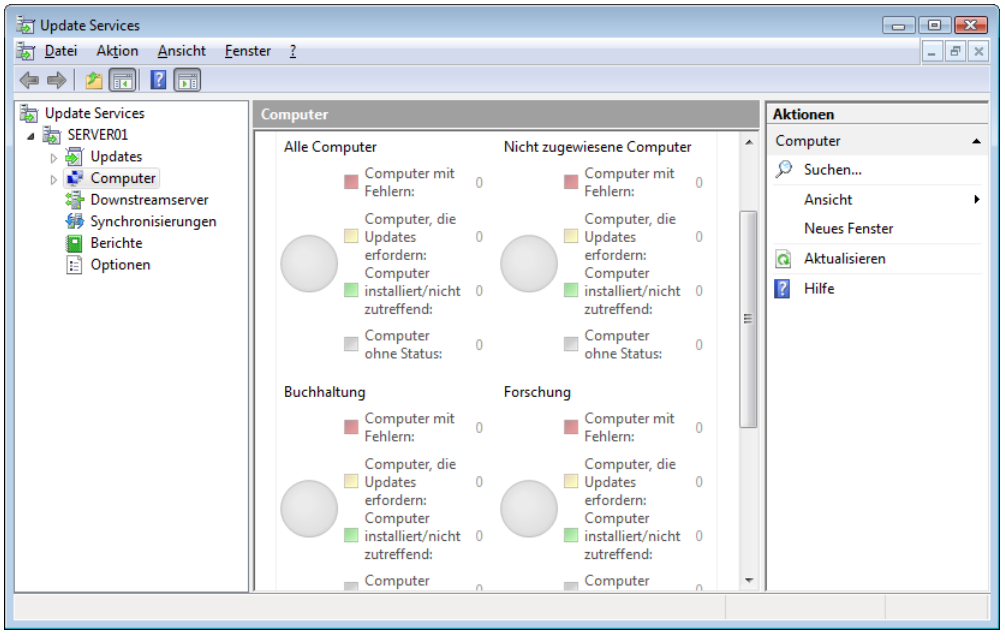


Abbildung 12.13 WSUS-Computergruppen

WSUS ermöglicht auch eine zentrale Deinstallation eines Updates auf allen Computern der Organisation. Wenn ein Update beispielsweise mit Windows Update installiert wurde und dann zu Problemen führt, müssen die Administratoren das Update auf jedem Computer der Organisation manuell deinstallieren und dann ausblenden. Verwendet die Organisation WSUS und es ergeben sich mit einem Update Probleme, kann der Updateadministrator die Installation in WSUS rückgängig machen. Dadurch wird das Update von allen Clientcomputern der Organisation entfernt. Es ist nicht erforderlich, das Update anschließend auszublenden, weil der WSUS-Server nur genehmigte Updates für die Windows Update-Clients verfügbar macht.



Weitere Informationen WSUS

Weitere Informationen über WSUS erhalten Sie im Windows Server Update Services-Tech-Center unter folgender Microsoft TechNet-Adresse: *http://technet.microsoft.com/de-de/wsus/default.aspx.*

Richtlinien für Windows Update

Auf der Seite *Windows Update* der Systemsteuerung können Sie zwar einige Einstellungen vornehmen und zum Beispiel festlegen, wann die Suche nach Updates erfolgen soll und was der Computer mit neuen Updates tun soll, aber die meisten Einstellungen für Windows Update erfolgen in den Gruppenrichtlinien. Der Knoten *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows Update* enthält 16 Richtlinien (Abbildung 12.14).

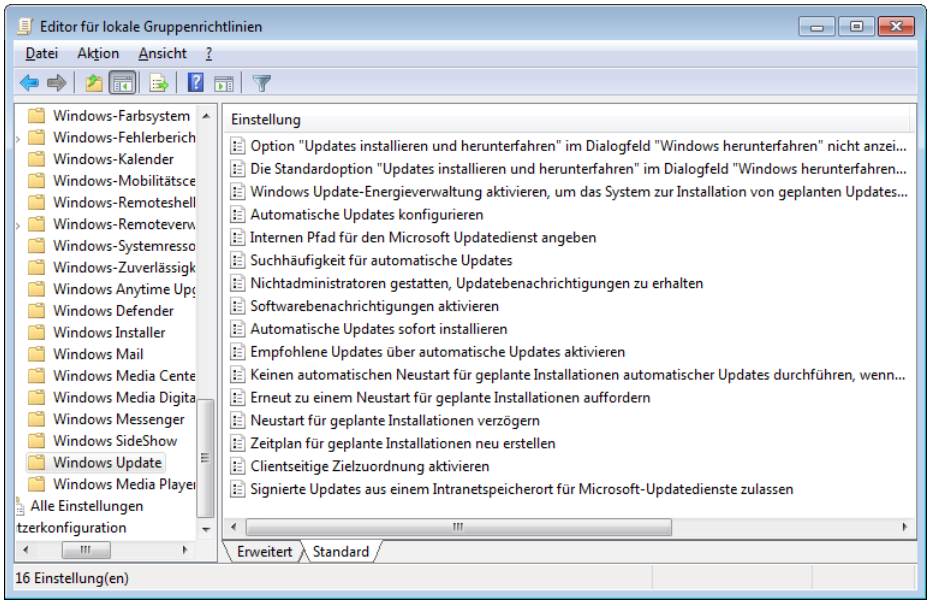


Abbildung 12.14 Richtlinien für Windows Update

Mit folgenden Richtlinien können Sie Windows Update konfigurieren:

- **Option "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anzeigen** Mit dieser Richtlinieneinstellung können Sie festlegen, ob im Dialogfeld *Windows herunterfahren* die Option *Updates installieren und herunterfahren* angezeigt wird. Standardmäßig wird diese Option angezeigt.
- **Die Standardoption "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anpassen** Wenn diese Richtlinie aktiviert ist, wird die letzte Wahl des Benutzers beim Herunterfahren als Standardoption verwendet. Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, wird die Option *Updates installieren und herunterfahren* als Standardoption verwendet, wenn Updates zur Installation bereitstehen. Die Richtlinie ist unwirksam, wenn die Richtlinie *Option "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anzeigen* aktiviert ist.

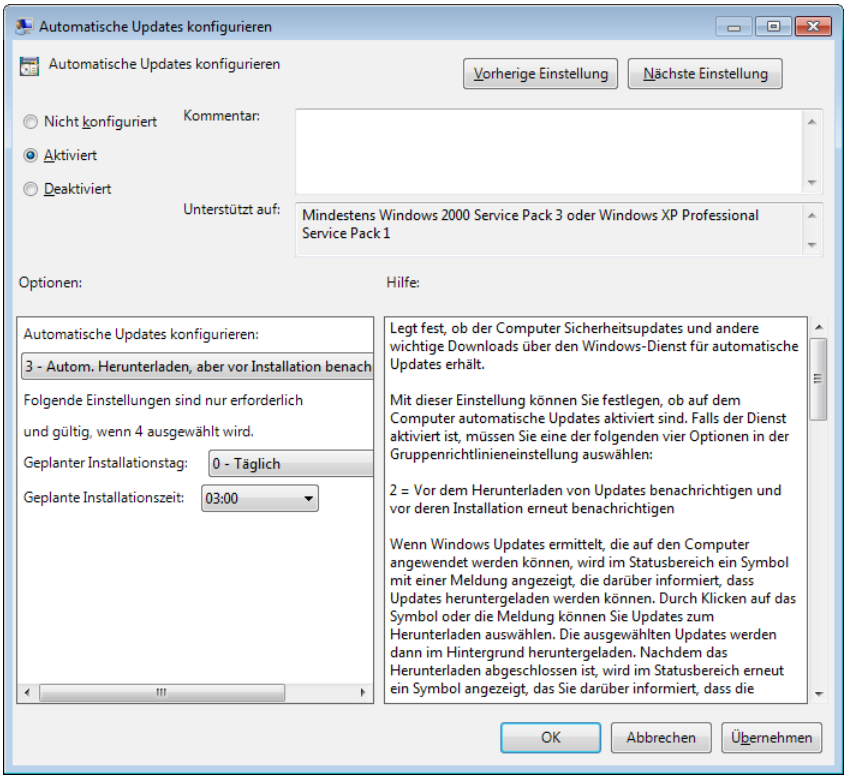

Automatische Updates konfigurieren
Automatische Updates konfigurieren
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows 2000 Service Pack 3 oder Windows XP Professional Service Pack 1
Optionen:
Hilfe:
Automatische Updates konfigurieren:
3 - Autom. Herunterladen, aber vor Installation benach
Folgende Einstellungen sind nur erforderlich
und gültig, wenn 4 ausgewählt wird.
Geplanter Installationstag:
0 - Täglich
Geplante Installationszeit:
03:00
Legt fest, ob der Computer Sicherheitsupdates und andere wichtige Downloads über den Windows-Dienst für automatische Updates erhält.
Mit dieser Einstellung können Sie festlegen, ob auf dem Computer automatische Updates aktiviert sind. Falls der Dienst aktiviert ist, müssen Sie eine der folgenden vier Optionen in der Gruppenrichtlinieneinstellung auswählen:
2 = Vor dem Herunterladen von Updates benachrichtigen und vor deren Installation erneut benachrichtigen
Wenn Windows Updates ermittelt, die auf den Computer angewendet werden können, wird im Statusbereich ein Symbol mit einer Meldung angezeigt, die darüber informiert, dass Updates heruntergeladen werden können. Durch Klicken auf das Symbol oder die Meldung können Sie Updates zum Herunterladen auswählen. Die ausgewählten Updates werden dann im Hintergrund heruntergeladen. Nachdem das Herunterladen abgeschlossen ist, wird im Statusbereich erneut ein Symbol angezeigt, das Sie darüber informiert, dass die
OK
Abbrechen
Übernehmen

Abbildung 12.15 Die Richtlinie *Automatische Updates konfigurieren*

- **Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivieren** Diese Richtlinie ermöglicht es Windows Update, den Computer aus dem Ruhezustand zu reaktivieren, um Updates zu installieren. Es werden keine Updates installiert, wenn der im Ruhezustand befindliche Computer durch einen Akku mit Strom versorgt wird.
- **Automatische Updates konfigurieren** Diese Richtlinie (Abbildung 12.15) ermöglicht Einstellungen für die Erkennung, das Herunterladen und die Installation von Updates. Einige der Einstellungen sind auch auf der Seite *Windows Update* der Systemsteuerung verfügbar. Mit dieser Richtlinie können Sie folgende Einstellungen vornehmen:
  - **Vor Herunterladen und Installation benachrichtigen** Windows Update lädt keine Updates herunter, sondern informiert den Benutzer nur darüber, dass Updates zum Herunterladen und Installieren verfügbar sind.
  - **Autom. Herunterladen, aber vor Installation benachrichtigen** Windows Update lädt Updates herunter und informiert den Benutzer darüber, dass Updates zur Installation bereitstehen.
  - **Autom. Herunterladen und laut Zeitplan installieren** Windows Update lädt Updates herunter und installiert sie. Ein Eingreifen des Benutzers ist nicht erforderlich.

- **Lokalen Administrator[en] ermöglichen, Einstellung auszuwählen** Diese Einstellung ermöglicht es lokalen Administratoren, in gewissem Umfang Einstellungen für Windows Update vorzunehmen und beispielsweise den Installationszeitpunkt festzulegen.
- **Installationstag und Installationszeit** Mit diesen Einstellungen können Sie den Tag und die Uhrzeit festlegen, zu der Updates von Windows Update installiert werden.

- **Internen Pfad für den Microsoft Updatedienst angeben** Diese Richtlinie ermöglicht die Angabe des internen Updateservers, beispielsweise eines WSUS-Servers (Abbildung 12.16). Die Richtlinie ist die einzige Möglichkeit, Windows Update so zu konfigurieren, dass es einen anderen Updateserver verwendet. Mit der Richtline können Sie den Updateserver und den Statistikserver festlegen. Für beides wird gewöhnlich derselbe Server verwendet. Der Updateserver ist der Server, von dem die Updates heruntergeladen werden, und der Statistikserver ist der Server, zu dem Clients Installationsinformationen hochladen.

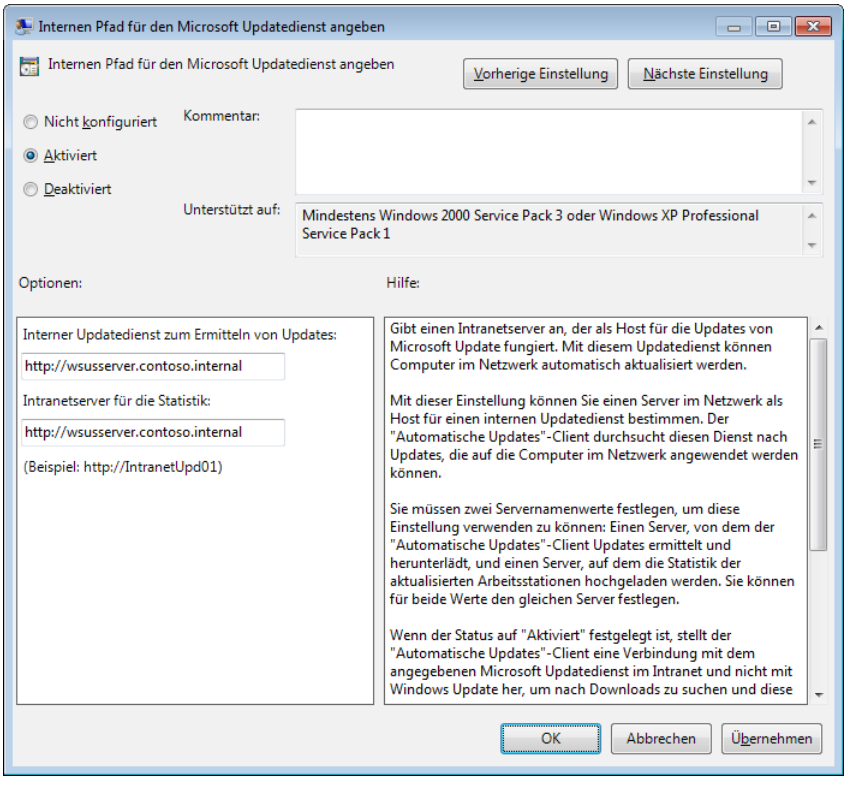

Internen Pfad für den Microsoft Updatedienst angeben
Internen Pfad für den Microsoft Updatedienst angeben
Vorherige Einstellung
Nächste Einstellung
Nicht konfiguriert
Aktiviert
Deaktiviert
Kommentar:
Unterstützt auf:
Mindestens Windows 2000 Service Pack 3 oder Windows XP Professional Service Pack 1
Optionen:
Hilfe:
Interner Updatedienst zum Ermitteln von Updates:
http://wsusserver.contoso.internal
Intranetserver für die Statistik:
http://wsusserver.contoso.internal
(Beispiel: http://IntranetUpd01)
Gibt einen Intranetserver an, der als Host für die Updates von Microsoft Update fungiert. Mit diesem Updatedienst können Computer im Netzwerk automatisch aktualisiert werden.
Mit dieser Einstellung können Sie einen Server im Netzwerk als Host für einen internen Updatedienst bestimmen. Der "Automatische Updates"-Client durchsucht diesen Dienst nach Updates, die auf die Computer im Netzwerk angewendet werden können.
Sie müssen zwei Servernamenwerte festlegen, um diese Einstellung verwenden zu können: Einen Server, von dem der "Automatische Updates"-Client Updates ermittelt und herunterlädt, und einen Server, auf dem die Statistik der aktualisierten Arbeitsstationen hochgeladen werden. Sie können für beide Werte den gleichen Server festlegen.
Wenn der Status auf "Aktiviert" festgelegt ist, stellt der "Automatische Updates"-Client eine Verbindung mit dem angegebenen Microsoft Updatedienst im Intranet und nicht mit Windows Update her, um nach Downloads zu suchen und diese
OK
Abbrechen
Übernehmen

Abbildung 12.16 Angeben des internen Updateservers

- **Suchhäufigkeit für automatische Updates** Mit dieser Richtlinie legen Sie fest, wie häufig Windows Update überprüft, ob auf dem Updateserver aus dem lokalen Intranet Updates vorliegen. Die Richtlinie ist unwirksam, wenn Sie den Client so konfigurieren, dass er Updates von den Windows Update-Servern anfordert.

- **Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten** Diese Richtlinie legt fest, ob Benutzer, die nicht zur lokalen Gruppe *Administratoren* gehören, Updates installieren können.
- **Softwarebenachrichtigungen aktivieren** Wenn Sie diese Richtlinie aktivieren, versorgt Windows Update die Benutzer mit Informationen über optionale Updates.
- **Automatische Updates sofort installieren** Wenn Sie diese Richtlinie aktivieren, werden Updates, die keinen Neustart des Computers erfordern, automatisch installiert. Updates, die einen Neustart erfordern, werden nicht installiert, bis die Bedingungen erfüllt sind, die in der Richtlinie *Automatische Updates konfigurieren* festgelegt wurden.
- **Empfohlene Updates über automatische Updates aktivieren** Mit dieser Richtlinie können Sie festlegen, dass Windows Update nicht nur wichtige Updates, sondern auch empfohlene Updates installiert.
- **Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind** Wenn Sie diese Richtlinie aktivieren, wartet Windows Update mit der Installation von Updates, die einen Neustart des Computers erfordern, bis sich der aktuell angemeldete Benutzer abmeldet. Wenn Sie diese Richtlinie deaktivieren oder nicht konfigurieren und die Richtlinie *Automatische Updates konfigurieren* so eingestellt ist, dass Updates zu einem bestimmten Zeitpunkt installiert werden, weist Windows Update den angemeldeten Benutzer 5 Minuten vorher auf den anstehenden Neustart hin.
- **Erneut zu einem Neustart für geplante Installationen auffordern** Mit dieser Richtlinie können Sie festlegen, wie lange ein Benutzer einen geplanten Neustart verzögern kann, wenn die Richtlinie *Automatische Updates konfigurieren* die Installation von Updates zu einem bestimmten Zeitpunkt vorsieht.
- **Neustart für geplante Installationen verzögern** Mit dieser Richtlinie können Sie festlegen, wie lange Windows nach einer geplanten Installation mit dem Neustart des Computers wartet. Die Richtlinie ist nur wirksam, wenn die Richtlinie *Automatische Updates konfigurieren* die Installation von Updates zu einem bestimmten Zeitpunkt vorsieht.
- **Zeitplan für geplante Installationen neu erstellen** Mit dieser Richtlinie können Sie festlegen, wie lange Windows Update nach dem Neustart eines Computers wartet, bis es ein Update durchführt, dessen Installation zum vorgesehenen Zeitpunkt verpasst wurde. Sie können zum Beispiel festlegen, dass ein Computer, der zum geplanten Zeitpunkt ausgeschaltet war, Updates 1 Minute nach dem Start installiert. Eine Deaktivierung der Richtlinie bedeutet, dass Updates zum nächsten geplanten Zeitpunkt installiert werden.
- **Clientseitige Zielzuordnung aktivieren** Mit dieser Richtlinie können Sie Computer verschiedenen Softwareupdategruppen zuordnen. Dadurch lassen sich Updates gezielt auf den ausgewählten Computern installieren und werden nicht auf allen Computern der Organisation installiert.
- **Signierte Updates aus einem Intranetspeicherort für Microsoft-Updatedienste zulassen** Mit dieser Richtlinie können Sie zulassen, dass Updates von anderen Herstellern vom Updateserver des Intranets heruntergeladen werden können, sofern sie von einem vertrauenswürdigen Herausgeber signiert wurden.

Microsoft Baseline Security Analyzer

Mit dem Tool Microsoft Baseline Security Analyzer (MBSA) können Sie überprüfen, ob auf Clientcomputern alle verfügbaren Softwareupdates installiert worden sind. Mit diesem Tool können Administratoren in Umgebungen, die keine zentrale Updatelösung wie WSUS verwenden, erkennen, welche Clients in Bezug auf Sicherheitsupdates nicht auf dem aktuellen Stand sind. Wenn Sie kein Hilfsprogramm wie das Tool MBSA verwenden, müssen Sie auf jedem Computer mit Windows Update überprüfen, ob alle Updates installiert wurden. Das MBSA-Tool wird in den späteren Stadien des Lebenszyklus eines Betriebssystems zunehmend wichtiger. Je länger ein Betriebssystem auf dem Markt ist, desto mehr Updates sind gewöhnlich für das Betriebssystem verfügbar und desto zeitaufwendiger wird die Überprüfung, ob bestimmte Updates fehlen.

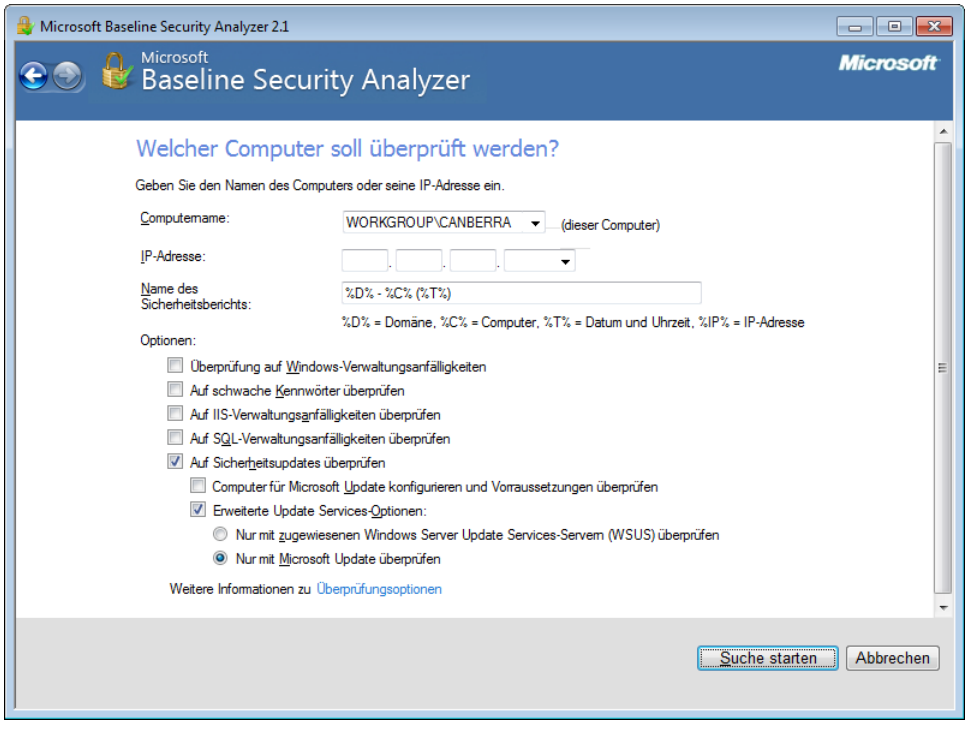


Abbildung 12.17 Microsoft Baseline Security Analyzer

Wie Abbildung 12.17 zeigt, kann das MBSA-Tool einen Computer anhand von Microsoft Update überprüfen, oder es kann einen Computer auf der Basis der Updates überprüfen, die auf einem WSUS-Server genehmigt wurden. Mit dem MBSA-Tool können Sie auch überprüfen, ob es Probleme mit der Sicherheitskonfiguration eines Computers gibt, weil zum Beispiel Anfälligkeiten in der Verwaltung bestehen oder unsichere Kennwörter verwendet werden. Mit dem MBSA-Tool können Sie nicht nur Clients überprüfen, sondern auch Server, beispielsweise auf Anfälligkeiten in den Internetinformationsdiensten oder im SQL-Server. Um Computer zu überprüfen, brauchen Sie auf dem lokalen Computer und auf jedem Remotecomputer, den Sie untersuchen, Administratorrechte. Dadurch ist sichergestellt, dass sich das MBSA-Tool nicht als Angriffswerkzeug eignet, mit dem die Computer anderer Leute

auf Schwachstellen untersucht werden können. Die Version 2.1 des MBSA-Tools und ältere Versionen eignen sich nicht für die Untersuchung von Windows 7-Computern.



Weitere Informationen MBSA

Weitere Informationen über MBSA erhalten Sie auf der folgenden Microsoft TechNet-Webseite: *http://technet.microsoft.com/de-de/security/cc184923.aspx*.



Prüfungstipp

Merken Sie sich die Funktion der Richtlinie *Internen Pfad für den Microsoft Updatedienst angeben*.

Übung Konfigurieren von Windows Update

In dieser Übung konfigurieren Sie Windows Update in der Systemsteuerung und mit dem Editor für lokale Gruppenrichtlinien.

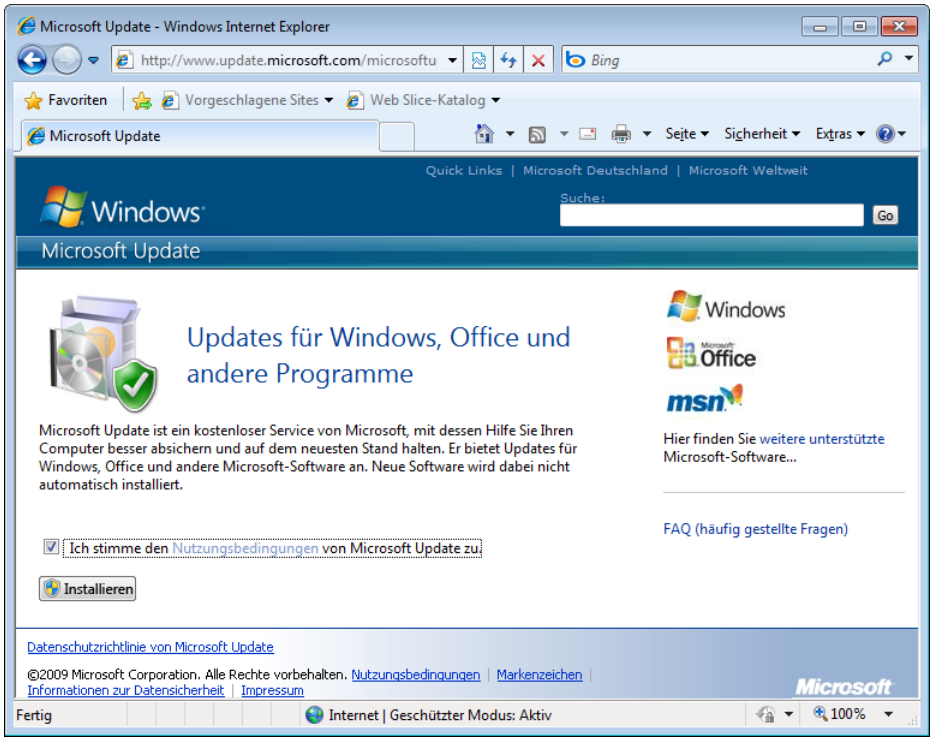

Microsoft Update - Windows Internet Explorer
http://www.update.microsoft.com/microsoftu
Bing
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Microsoft Update
Seite
Sicherheit
Extras
Quick Links | Microsoft Deutschland | Microsoft Weltweit
Windows
Suche:
Go
Microsoft Update
Updates für Windows, Office und andere Programme
Microsoft Update ist ein kostenloser Service von Microsoft, mit dessen Hilfe Sie Ihren Computer besser absichern und auf dem neuesten Stand halten. Er bietet Updates für Windows, Office und andere Microsoft-Software an. Neue Software wird dabei nicht automatisch installiert.
Windows
Office
msn
Hier finden Sie weitere unterstützte Microsoft-Software...
FAQ (häufig gestellte Fragen)
Ich stimme den Nutzungsbedingungen von Microsoft Update zu.
Installieren
Datenschutzrichtlinie von Microsoft Update
©2009 Microsoft Corporation. Alle Rechte vorbehalten. Nutzungsbedingungen | Markenzeichen | Informationen zur Datensicherheit | Impressum
Microsoft
Fertig
Internet | Geschützter Modus: Aktiv
100%

Abbildung 12.18 Es sind weitere Updates verfügbar

Übung 1 Konfigurieren von Windows Update in der Systemsteuerung

In dieser Übung richten Sie Windows Update so ein, dass es nicht nur für das Betriebssystem und die Standardanwendungen aus dem Lieferumfang des Betriebssystems Updates anfordert, sondern auch für andere Microsoft-Anwendungen, wie zum Beispiel Office. Für diese Übung muss der Computer *Canberra* über Internetzugang verfügen:

1. Melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Windows Update** ein und drücken Sie die EINGABETASTE.
3. Klicken Sie auf der Seite *Windows Update* der Systemsteuerung auf das Element *Weitere Informationen* neben dem Text *Rufen Sie Updates für weitere Microsoft-Produkte ab*. Dadurch öffnet sich ein Webbrowserfenster (Abbildung 12.18).
4. Wählen Sie das Kontrollkästchen *Ich stimme den Nutzungsbedingungen von Microsoft Update zu* und klicken Sie dann auf *Installieren*. Wenn sich die Benutzerkontensteuerung meldet, klicken Sie auf *Ja*.
5. Schließen Sie das Webbrowserfenster. Klicken Sie auf der Seite *Windows Update* der Systemsteuerung auf die Schaltfläche *Einstellungen ändern*.
6. Überprüfen Sie, ob das Kontrollkästchen *Updates für Microsoft-Produkte beim Ausführen von Windows Update bereitstellen und nach neuer optionaler Microsoft-Software suchen* vorhanden und aktiviert ist.
7. Stellen Sie mit den Dropdownlisten den Installationstag auf *Jeden Freitag* ein und den Zeitpunkt auf 17 Uhr. Überprüfen Sie die Einstellungen anhand von Abbildung 12.19 und klicken Sie dann auf *OK*. Schließen Sie die Systemsteuerung.

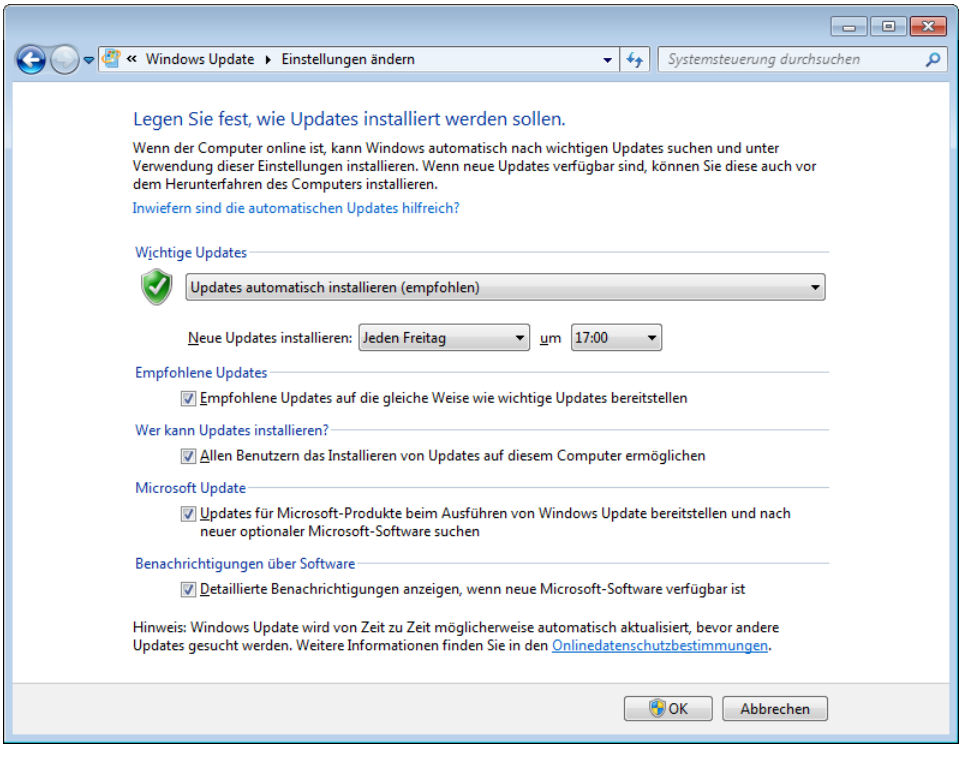

« Windows Update ▸ Einstellungen ändern
Systemsteuerung durchsuchen
Legen Sie fest, wie Updates installiert werden sollen.
Wenn der Computer online ist, kann Windows automatisch nach wichtigen Updates suchen und unter Verwendung dieser Einstellungen installieren. Wenn neue Updates verfügbar sind, können Sie diese auch vor dem Herunterfahren des Computers installieren.
Inwiefern sind die automatischen Updates hilfreich?
Wichtige Updates
Updates automatisch installieren (empfohlen)
Neue Updates installieren: Jeden Freitag um 17:00
Empfohlene Updates
Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen
Wer kann Updates installieren?
Allen Benutzern das Installieren von Updates auf diesem Computer ermöglichen
Microsoft Update
Updates für Microsoft-Produkte beim Ausführen von Windows Update bereitstellen und nach neuer optionaler Microsoft-Software suchen
Benachrichtigungen über Software
Detaillierte Benachrichtigungen anzeigen, wenn neue Microsoft-Software verfügbar ist
Hinweis: Windows Update wird von Zeit zu Zeit möglicherweise automatisch aktualisiert, bevor andere Updates gesucht werden. Weitere Informationen finden Sie in den Onlinedatenschutzbestimmungen.
OK
Abbrechen

Abbildung 12.19 Überprüfen der Einstellungen für diese Übung

Übung 2 Konfigurieren von Windows Update mit Gruppenrichtlinien

Im Editor für lokale Gruppenrichtlinien können Sie einige Einstellungen für Windows Update vornehmen, die sich nicht in der Systemsteuerung vornehmen lassen. In dieser Übung richten Sie einen Computer so ein, dass er aus seinem Ruhezustand erwacht, wenn der vorgesehene Zeitpunkt für die Suche nach Updates gekommen ist. Sie lassen die automatische Installation von Updates zu, die keinen Neustart erfordern, und sorgen dafür, dass kein automatischer Neustart durchgeführt wird, wenn ein Benutzer am Computer angemeldet ist:

1. Sofern Sie es noch nicht getan haben, melden Sie sich mit dem Benutzerkonto *Kim_Akers* auf dem Computer *Canberra* an.
2. Geben Sie im Textfeld *Programme/Dateien durchsuchen* **Gpedit.msc** ein und drücken Sie die EINGABETASTE. Der Editor für lokale Gruppenrichtlinien öffnet sich.
3. Navigieren Sie zum Knoten *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows Update*.
4. Aktivieren Sie die Richtlinie *Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivieren*.
5. Aktivieren Sie die Richtlinie *Automatische Updates sofort installieren*.
6. Aktivieren Sie die Richtlinie *Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind*.
7. Schließen Sie den Editor für lokale Gruppenrichtlinien, geben Sie im Textfeld *Programme/Dateien durchsuchen* **gpupdate /force** ein und drücken Sie die EINGABETASTE.

Zusammenfassung der Lektion

- Windows Update ermöglicht es, Softwareupdates automatisch von den Microsoft Update-Servern oder einer lokalen Updatequelle, beispielsweise einem WSUS-Server, auf Windows 7-Clients herunterzuladen und zu installieren.
- Sie können Windows Update so konfigurieren, dass Updates automatisch heruntergeladen und installiert werden. Windows Update lässt sich auch so konfigurieren, dass Updates heruntergeladen und der angemeldete Benutzer über die Verfügbarkeit der Updates informiert wird, oder dass der angemeldete Benutzer nur darüber informiert wird, dass Updates heruntergeladen und installiert werden können.
- Standardbenutzer können mit Windows Update nach Updates suchen und sie installieren. Nur Benutzer mit Administratorrechten können die Einstellungen von Windows Update ändern oder die Updatequelle von Microsoft Update auf einen lokalen WSUS-Server umstellen.
- Benutzer mit Administratorrechten können Updates ausblenden. Ein ausgeblendetes Update wird nicht auf dem Computer installiert. Ein ausgeblendetes Update kann später wieder eingeblendet und installiert werden. Benutzer mit Administratorrechten können installierte Updates deinstallieren. Ein deinstalliertes Update wird wieder für die Installation verfügbar, außer es wird von einem Administrator ausgeblendet.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zum Stoff aus Lektion 1, »Aktualisieren von Windows 7«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf die Fragen und Erläuterungen, warum die entsprechende Antwort richtig oder falsch ist, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welche der folgenden Aufgaben kann ein Standardbenutzer in Windows Update ausführen, wenn Windows 7 mit den Standardeinstellungen konfiguriert wurde?
   A. Updates deinstallieren
   B. Updates installieren
   C. Installationszeitpunkt von Updates ändern
   D. Verhalten in Bezug auf das Herunterladen und Installieren von Updates ändern
   E. Updates ausblenden
2. Sie haben gerade festgestellt, dass ein Update, das letzte Woche über Windows Update verfügbar geworden ist und als wichtig eingestuft wird, nach der Installation auf Windows 7-Clients zu einem Konflikt mit einer Anwendung führt, die für die tägliche Arbeit Ihrer Organisation wichtig ist. Dieser Konflikt verhindert, dass sich die Anwendung verwenden lässt. Sie haben mit dem Hersteller der Anwendung gesprochen, der Ihnen versichert hat, dass innerhalb von 2 Monaten eine Lösung verfügbar sein wird. Die Windows 7-Clients wurden alle mit den Standardeinstellungen für Windows Update konfiguriert. Wie erreichen Sie nun, dass sich die benutzerdefinierte Anwendung wieder verwenden lässt und dass Standardbenutzer das Update nicht installieren können, bevor die Lösung des Herstellers verfügbar ist? Andere wichtige Updates, die über Windows Update verfügbar werden, sollten aber weiterhin installiert werden. (Wählen Sie alle zutreffenden Antworten; jede richtige Antwort ist Teil der vollständigen Lösung.)
   A. Sie ändern die Updateeinstellungen
   B. Sie deinstallieren das Update
   C. Sie blenden das Update aus
   D. Sie installieren das Update
3. Sie haben die geplanten Updates zwar so konfiguriert, dass sie während der Mittagspause erfolgen, mussten dann aber feststellen, dass ein beträchtlicher Teil der Computer in diesem Zeitraum gar nicht eingeschaltet ist. Nun möchten Sie sicherstellen, dass die geplanten Updates nachgeholt werden, sobald die Computer wieder eingeschaltet werden. Welche der folgenden Richtlinien sollten Sie dafür konfigurieren?
   A. *Erneut zu einem Neustart für geplante Installationen auffordern*
   B. *Neustart für geplante Installationen verzögern*
   C. *Zeitplan für geplante Installationen neu erstellen*

D. *Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind*

4. Welche der folgenden Richtlinien sollten Sie konfigurieren, wenn ein Windows 7-Client als Updatequelle den WSUS-Server *updates.contoso.internal* verwenden soll und nicht die Microsoft Update-Server?
   A. *Softwarebenachrichtigungen aktivieren*
   B. *Suchhäufigkeit für automatische Updates*
   C. *Automatische Updates konfigurieren*
   D. *Internen Pfad für den Microsoft Updatedienst angeben*
5. Sie verwalten in einer Organisation, die keinen WSUS-Server verwendet, 30 separate Windows 7-Clients. Alle Clients sind Mitglieder einer Domäne, die mit den Active Directory-Domänendiensten von Windows Server 2008 aufgebaut wurde. Mit welchem der folgenden Tools können Sie überprüfen, ob auf diesen Computern ein bestimmtes Softwareupdate fehlt?
   A. Microsoft Update
   B. WSUS
   C. Gruppenrichtlinienverwaltungskonsole
   D. MBSA

Lektion 2: Konfigurieren von Internet Explorer

Es gibt zwar kostenlose Alternativen, aber der Internet Explorer ist der unter Windows am häufigsten eingesetzte Browser. Sehr viele Einstellungen machen den Internet Explorer flexibel konfigurierbar, aber auf einen unerfahrenen Administrator wirkt diese Fülle an Einstellmöglichkeiten auch etwas einschüchternd. In dieser Lektion lernen Sie die Einzelheiten der Internet Explorer-Konfiguration kennen, die festlegen, wie Seiten in der Kompatibilitätsansicht dargestellt werden. Sie konfigurieren die Sicherheitseinstellungen des Internet Explorers und von Add-Ons, die den Funktionsumfang des Browsers erweitern. Darüber hinaus verwalten Sie Zertifikate und das InPrivate-Browsen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Konfigurieren der Kompatibilitätsansicht im Internet Explorer
- Konfigurieren der Sicherheitseinstellungen des Internet Explorers
- Konfigurieren von Anbietern im Internet Explorer
- Verwalten von Add-Ons im Internet Explorer
- Steuern des InPrivate-Modus
- Verwalten von Zertifikaten für sichere Websites

Veranschlagte Zeit für diese Lektion: 40 Minuten

Die Kompatibilitätsansicht im Internet Explorer

Die Kompatibilitätsansicht des Internet Explorers ermöglicht es, Sites, die für Vorgängerversionen von Internet Explorer entworfen wurden, im Internet Explorer 8 darzustellen, wie es vorgesehen war. Sie aktivieren die Kompatibilitätsansicht für eine Seite, indem Sie am Ende der Adressleiste das Symbol mit der zerrissenen Seite anklicken. Die Einstellungen für die Kompatibilitätsansicht konfigurieren Sie im Dialogfeld *Einstellungen der Kompatibilitätsansicht*, das Sie öffnen, indem Sie im Menü *Extras* des Internet Explorers den Befehl *Einstellungen der Kompatibilitätsansicht* wählen.

In diesem Dialogfeld können Sie festlegen, dass der Internet Explorer die Kompatibilitätsansicht automatisch für eine Liste von Websites verwendet, die über Windows Update verteilt wird. Diese Liste enthält beliebte Websites, die in der Kompatibilitätsansicht besser funktionieren, sowie andere Websites, die ihre Details an Microsoft übermittelt haben. In der Standardeinstellung zeigt der Internet Explorer alle Intranetsites in der Kompatibilitätsansicht an. Was Intranetsites sind, wird durch die *Zone Lokales Intranet* festgelegt. Über Zonen erfahren Sie mehr weiter unten in dieser Lektion. Sie können die Kompatibilitätsansicht für Intranetsites im Dialogfeld *Einstellungen der Kompatibilitätsansicht* deaktivieren. Außerdem können Sie den Internet Explorer in diesem Dialogfeld so konfigurieren, dass er bestimmte Websites in der Kompatibilitätsansicht anzeigt. Abbildung 12.20 zeigt, wie der Internet Explorer so konfiguriert wird, dass er die Website *contoso.com* in der Kompatibilitätsansicht darstellt. Sie können den Internet Explorer auch zwingen, alle Websites in der Kompatibilitätsansicht anzuzeigen; aktivieren Sie dazu das Kontrollkästchen *Alle Websites in Kompatibilitätsansicht anzeigen*.

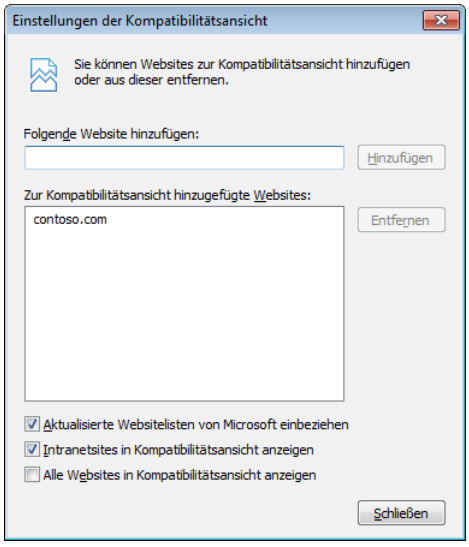


Abbildung 12.20 Einstellungen der Kompatibilitätsansicht

Gruppenrichtlinien im Zusammenhang mit der Kompatibilitätsansicht befinden sich im Knoten *Administrative Vorlagen\Windows-Komponenten\Internet Explorer\Kompatibilitätsansicht* sowohl unter *Computerkonfiguration* als auch unter *Benutzerkonfiguration*. Diese Richtlinien haben folgende Bedeutugn:

- **Internet Explorer 7-Standards-Modus aktivieren** Wenn Sie diese Richtlinie aktivieren, zeigt der Internet Explorer alle Websites in der Kompatibilitätsansicht an.
- **Kompatibilitätsansicht deaktivieren** Mit dieser Richtlinie deaktivieren Sie die Kompatibilitätsansicht.
- **Schaltfläche "Kompatibilitätsansicht" deaktivieren** Mit dieser Richtlinie können Sie die Schaltfläche *Kompatibilitätsansicht* deaktivieren.
- **Aktualisierte Websitelisten von Microsoft einbeziehen** Konfiguriert die Kompatibilitätsansicht so, dass sie eine aktualisierte Liste mit Sites auswertet, die von Microsoft über Windows Update veröffentlicht wird.
- **Richtlinienliste von Internet Explorer 7-Sites verwenden** Diese Richtlinie führt die Sites auf, für die der Internet Explorer die Kompatibilitätsansicht verwendet. Benutzer können Sites über das Dialogfeld *Einstellungen der Kompatibilitätsansicht* hinzufügen, aber keine Einträge der Standardsiteliste löschen.

Konfigurieren von Sicherheitseinstellungen

Sie können im Internet Explorer für unterschiedliche Websitetypen unterschiedliche Sicherheitsebenen konfigurieren. Dazu werden die Websites in Sicherheitszonen eingeteilt. Welche Sicherheitseinstellungen der Internet Explorer für eine Website verwendet, hängt von der entsprechenden Sicherheitszone ab. Es stehen folgende Sicherheitszonen zur Auswahl:

- **Lokales Intranet** Sites in der Zone *Lokales Intranet* sind Computer im Netzwerk Ihrer Organisation. Der Internet Explorer kann so konfiguriert werden, dass er Intranetsites automatisch erkennt. Sie können außerdem Websites zu dieser Zone hinzufügen,

wenn Sie im Dialogfeld *Lokales Intranet* auf die Schaltfläche *Erweitert* klicken (Abbildung 12.21). Die Standardsicherheitsstufe für diese Zone ist *Niedrig*. Der geschützte Modus ist für Sites in dieser Zone standardmäßig nicht aktiviert.

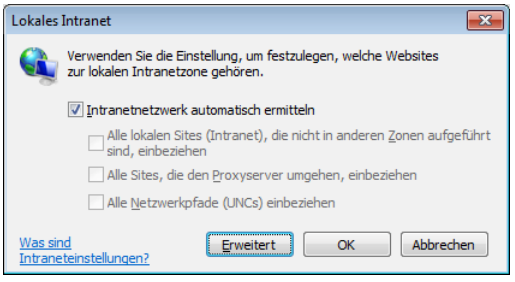

Lokales Intranet
Verwenden Sie die Einstellung, um festzulegen, welche Websites zur lokalen Intranetzone gehören.
Intranetnetzwerk automatisch ermitteln
Alle lokalen Sites (Intranet), die nicht in anderen Zonen aufgeführt sind, einbeziehen
Alle Sites, die den Proxyserver umgehen, einbeziehen
Alle Netzwerkpfade (UNCs) einbeziehen
Was sind Intraneteinstellungen?
Erweitert
OK
Abbrechen

Abbildung 12.21 Dialogfeld *Lokales Intranet*

- **Vertrauenswürdige Sites** Sites in der Zone *Vertrauenswürdige Sites* benötigen oft erhöhte Privilegien. Nur ausgewählte Websites sollten zu dieser Zone hinzugefügt werden, weil der Internet Explorer für die Sites aus dieser Zone weniger Sicherheitsmaßnahmen anwendet. Die Standardsicherheitsstufe für diese Zone ist *Mittel*. Der geschützte Modus ist für Sites in dieser Zone nicht standardmäßig aktiviert. Sie fügen Sites im Dialogfeld *Vertrauenswürdige Sites* hinzu. Die Standardeinstellung erfordert, dass alle Sites in der Zone *Vertrauenswürdige Sites* mit einem SSL-Zertifikat (Secure Sockets Layer) geschützt sind.
- **Eingeschränkte Sites** Sites in dieser Zone sind potenziell böswillig. Sie sollten nur Sites zu dieser Zone hinzufügen, wenn es nötig ist, gefährliche Websites zu besuchen. Die Standardsicherheitsstufe für diese Zone ist *Hoch*. Der geschützte Modus des Internet Explorers ist für Sites in diese Zone standardmäßig aktiviert.
- **Internet** Diese Zone umfasst alle Websites, die nicht in den Zonen *Lokales Intranet*, *Vertrauenswürdige Sites* oder *Eingeschränkte Sites* enthalten sind. Bei Sites in dieser Zone wird die Anzeige persönlicher Daten aus anderen Websites blockiert. Sites in dieser Zone dürfen keine Änderungen an Windows 7 durchführen. Die Standardsicherheitsstufe für diese Zone ist *Mittelhoch*. Der geschützte Modus ist für Sites in dieser Zone standardmäßig aktiviert.

Mit dem Schieberegler können Sie die Sicherheitsstufe ändern, die einer Zone zugewiesen ist (Abbildung 12.22). Sie können auch konfigurieren, ob eine Zone den geschützten Modus verwendet, und benutzerdefinierte Zoneneinstellungen wählen. Der geschützte Modus (protected mode) ist eine Technik, die den Internet Explorer zwingt, als Prozess mit geringer Integrität zu laufen. Die Sicherheitsarchitektur von Windows 7 sorgt dafür, dass Prozesse, denen eine geringe Integrität zugewiesen ist, daran gehindert werden, direkt mit Objekten zu kommunizieren, die einen höheren Integritätswert haben. Das bedeutet, dass Malware, der es gelingt, den Browser zu kompromittieren, daran gehindert wird, Windows 7 zu beschädigen. Als Prozess mit ebenfalls geringer Integrität kann die Malware nämlich keine Schäden verursachen. Der Entwurf von Windows 7 erlaubt es auch, die Prozesse, die in jeder Registerkarte laufen, voneinander zu trennen. Eine Registerkarte, in der eine Website im geschützten Modus läuft, kann somit gleichzeitig mit einer Registerkarte geöffnet werden, deren Site nicht im geschützten Modus ausgeführt wird. Sites, denen Sie nicht vertrauen, beispielsweise

Sites aus den Zonen *Internet* oder *Eingeschränkte Sites*, werden im geschützten Modus ausgeführt.

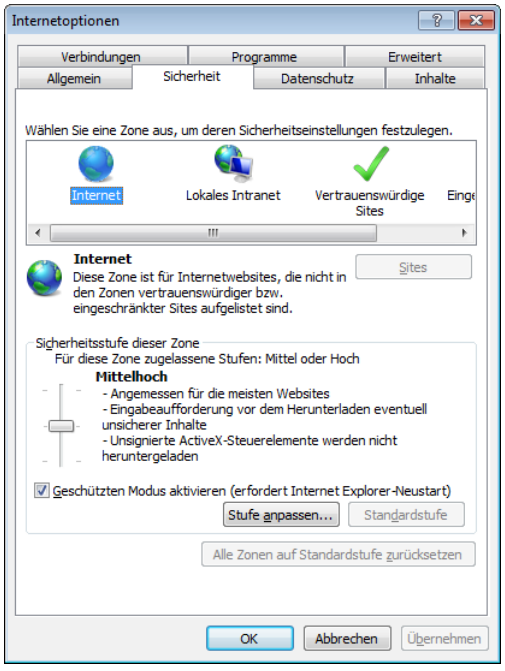


Abbildung 12.22 Registerkarte *Sicherheit* im Dialogfeld *Internetoptionen*

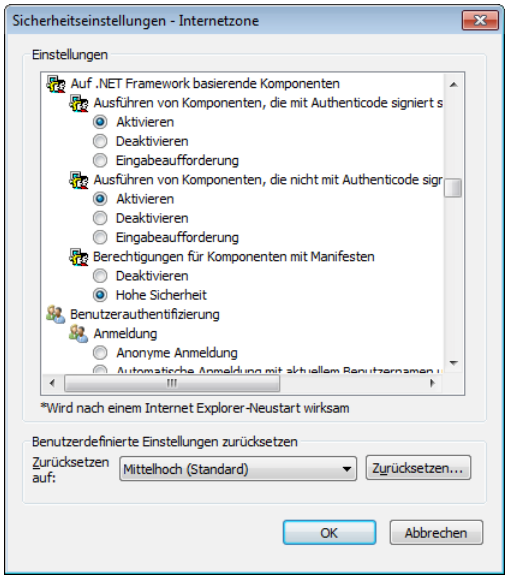


Abbildung 12.23 Benutzerdefinierte Einstellungen für die Sicherheitsstufen

Die drei Standardsicherheitsstufen sind *Mittel*, *Mittelhoch* und *Hoch*. Die Stufen werden immer restriktiver, wobei *Hoch* am stärksten eingeschränkt ist. Mit der Schaltfläche *Stufe anpassen* (Abbildung 12.23) können Sie die Sicherheit für eine Zone individuell konfigurieren. Zu den Elementen, die Sie hier konfigurieren, gehören unter anderem das Verhalten von ActiveX-Steuerelementen, Skripting und Einstellungen für die Benutzerauthentifizierung. Sofern Ihre Organisation nicht außergewöhnlich hohe Sicherheitsanforderungen hat, müssten die Standardsicherheitsstufen eigentlich ausreichen.

Auf der Registerkarte *Erweitert* des Dialogfelds *Internetoptionen* können Sie erweiterte Sicherheitsoptionen konfigurieren (Abbildung 12.24). Hier legen Sie zum Beispiel fest, ob der Internet Explorer Zertifikatsperrungsprüfungen durchführt, ob der SmartScreen-Filter in der Standardeinstellung aktiviert ist, welche Versionen von SSL und TLS (Transport Layer Security) unterstützt werden, ob die Windows-Authentifizierung unterstützt wird und ob der Internet Explorer eine Warnung anzeigt, wenn SSL-Zertifikat und Websiteadresse nicht übereinstimmen. Über die Konfiguration von SSL-Zertifikaten und SmartScreen-Filter erfahren Sie weiter unten in dieser Lektion mehr.

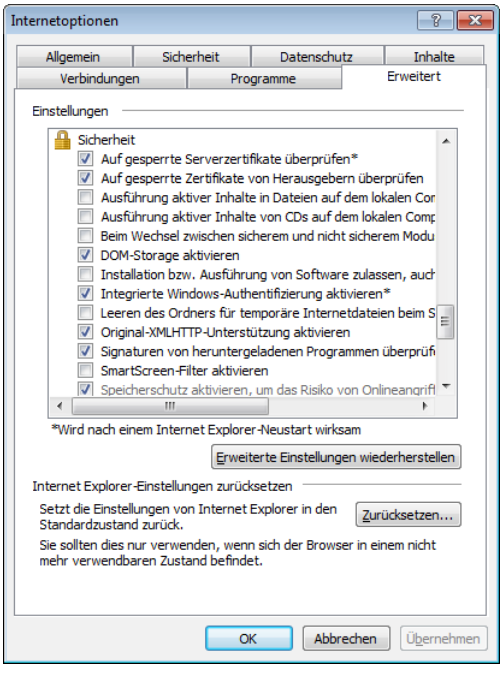


Abbildung 12.24 Erweiterte Sicherheitseinstellungen



Weitere Informationen **Verstärkte Sicherheitskonfiguration für den Internet Explorer**

Über die Ausführung des Internet Explorers mit verstärkten Sicherheitseinstellungen finden Sie auf der folgenden Microsoft TechNet-Webseite ausführliche Informationen: *http://technet.microsoft.com/de-de/library/dd883248.aspx*.

SmartScreen-Filter

Der SmartScreen-Filter ist ein Feature des Internet Explorers, das den Aufruf von Websites verhindert, von denen bekannt ist, dass sie Malware hosten oder dem Phishing dienen. *Phishing* bedeutet, dass Kriminelle eine Website einrichten, die eine Site nachahmt, die ein Benutzer regelmäßig besucht, etwa die Website einer Bank. Das Ziel dieser Aktion besteht darin, den Benutzer zu veranlassen, sich mit seinen Anmeldeinformationen zu authentifizieren. Der SmartScreen-Filter schützt Benutzer mit folgenden Techniken:

- **Analysiert besuchte Webseiten daraufhin, ob sie verdächtige Merkmale enthalten** Falls eine Webseite als verdächtig eingestuft wird, zeigt der SmartScreen-Filter eine Meldung an, die Sie auffordert, vorsichtig zu sein.
- **Vergleicht die besuchten Sites mit einer regelmäßig aktualisierten Liste bekannter Phishing- und Malwaresites** Wenn Sie eine Site aufrufen, die in dieser Liste aufgeführt ist, blockiert der SmartScreen-Filter die Anzeige mit einer Warnung vor dem gefährlichen Inhalt der Site.
- **Prüft heruntergeladene Dateien, die Sie von Websites herunterladen, auf bekannte Malware** Der SmartScreen-Filter zeigt eine Warnung an, dass der Download aus Sicherheitsgründen blockiert wurde.

Sie können eine Website von Hand prüfen, wenn Sie Ihnen verdächtig vorkommt. Wählen Sie dazu im Menü *Sicherheit* das Untermenü *SmartScreen-Filter* und darin den Befehl *Diese Website überprüfen*. Es öffnet sich das Dialogfeld *SmartScreen-Filter* (Abbildung 12.25). Mit dem Befehl *Unsichere Website melden* können Sie eine Website melden, von der Sie glauben, dass sie Malware hostet oder für Phishing eingesetzt wird. Die Website wird dann von Microsoft geprüft und bei Bedarf zur Liste gefährlicher Websites hinzugefügt.

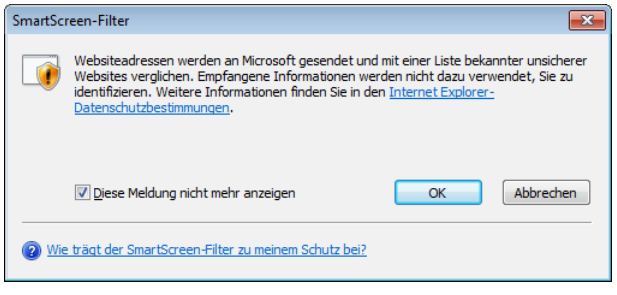

SmartScreen-Filter
Websiteadressen werden an Microsoft gesendet und mit einer Liste bekannter unsicherer Websites verglichen. Empfangene Informationen werden nicht dazu verwendet, Sie zu identifizieren. Weitere Informationen finden Sie in den Internet Explorer-Datenschutzbestimmungen.
Diese Meldung nicht mehr anzeigen
OK
Abbrechen
Wie trägt der SmartScreen-Filter zu meinem Schutz bei?

Abbildung 12.25 SmartScreen-Filter

Verwalten des InPrivate-Modus

Der InPrivate-Modus besteht aus zwei Technologien: *InPrivate-Filterung* und *InPrivate-Browsen*. Beide sind Datenschutztechnologien, die einschränken, wie viele Informationen über die Browsersitzung des Benutzers zur Verfügung gestellt werden. InPrivate-Browsen legt fest, welche Daten vom Browser gesammelt werden, und InPrivate-Filterung schränkt ein, welche Informationen über eine Browsersitzung von externen Dritten verfolgt werden können.

Benutzer öffnen ein Fenster für das InPrivate-Browsen, indem Sie im Menü *Sicherheit* den Befehl *InPrivate-Browsen* wählen. Während der Internet Explorer im InPrivate-Modus arbeitet, wird ein entsprechender Hinweis in der Adressleiste angezeigt (Abbildung 12.26).

Das InPrivate-Symbol erinnert den Benutzer daran, dass der Internet Explorer seine Browsingdaten nicht speichert. Sie sollten die Benutzer darüber aufklären, dass die Organisation ihre Browsingaktivitäten trotzdem mit anderen Methoden, etwa Auswertung der Proxyprotokolle, nachvollziehen kann, selbst wenn die Browserdaten nicht lokal aufgezeichnet werden.

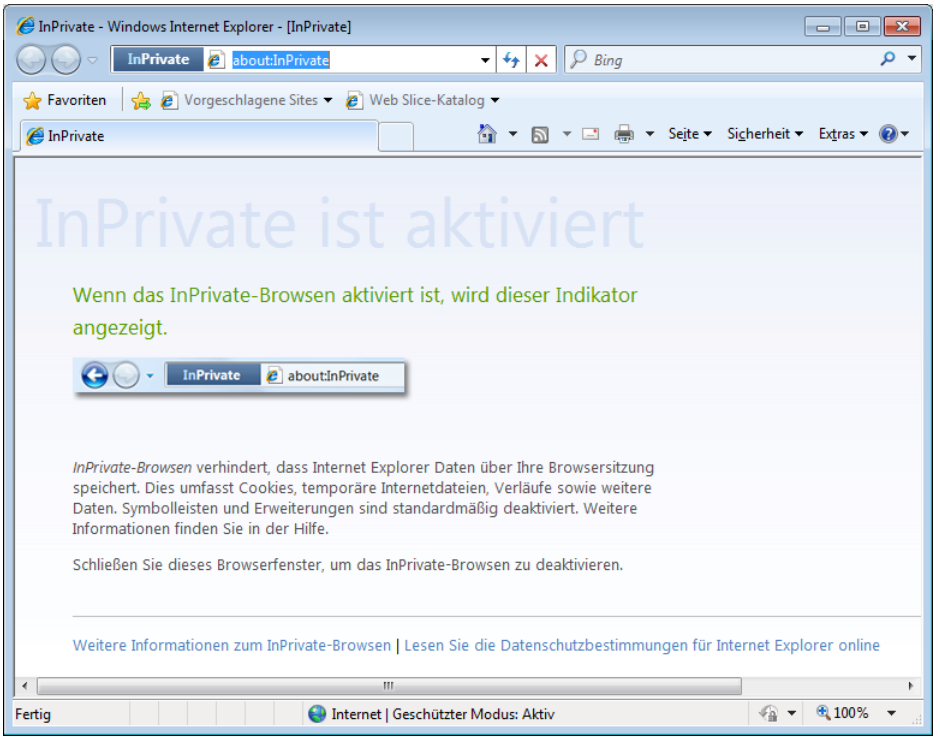

InPrivate - Windows Internet Explorer - [InPrivate]
InPrivate
about:InPrivate
Bing
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
InPrivate
Seite
Sicherheit
Extras
InPrivate ist aktiviert
Wenn das InPrivate-Browsen aktiviert ist, wird dieser Indikator angezeigt.
InPrivate
about:InPrivate
InPrivate-Browsen verhindert, dass Internet Explorer Daten über Ihre Browsersitzung speichert. Dies umfasst Cookies, temporäre Internetdateien, Verläufe sowie weitere Daten. Symbolleisten und Erweiterungen sind standardmäßig deaktiviert. Weitere Informationen finden Sie in der Hilfe.
Schließen Sie dieses Browserfenster, um das InPrivate-Browsen zu deaktivieren.
Weitere Informationen zum InPrivate-Browsen | Lesen Sie die Datenschutzbestimmungen für Internet Explorer online
Fertig
Internet | Geschützter Modus: Aktiv
100%

Abbildung 12.26 InPrivate-Browsen

Daten über das Webbrowsing werden gespeichert, während die InPrivate-Sitzung läuft. So können sich Benutzer beispielsweise bei ihrem Webmailkonto anmelden, wobei die erforderlichen Cookies temporär im Rahmen der InPrivate-Sitzung gespeichert werden. Sie können auch durch die Seiten zurücknavigieren, die sie bisher während der Sitzung besucht haben. Der Vorteil des InPrivate-Modus liegt darin, dass all diese Daten automatisch gelöscht werden, sobald das Browserfenster geschlossen wird. Es ist zwar möglich, einen Teil des Browserverlaufs mit dem Befehl *Browserverlauf löschen* aus dem Menü *Sicherheit* zu löschen, wie die Übung am Ende dieser Lektion demonstriert, aber dabei werden nicht alle Daten beseitigt.

Viele Webseiten binden Inhalt aus anderen Websites in ihre Seiten ein. So werden Werbebanner nur selten von der Website produziert, die Sie besuchen. Meist werden sie von einem anderen Unternehmen vermittelt. Wenn Sie eine Website besuchen, die auf diese Weise konfiguriert ist, werden einige Daten über Ihren Besuch an das Werbeunternehmen zurückgemeldet. Wenn Sie mehrere Sites besuchen, die vom selben Werbeunternehmen bedient werden, kann dieses Unternehmen die Daten über Ihre Besuche auf unterschiedlichen Websites zusammenführen, auf denen es Werbung schaltet. Nehmen wir an, dasselbe Unternehmen liefert Werbebanner für die separaten Sites A, B und C. Wenn Sie die Sites A, B und C be-

suchen, werden Daten an das Unternehmen zurückgesendet, die einiges über Ihre Vorlieben beim Webbrowsen verraten. Diese Methode beschränkt sich nicht auf Werbung, sie lässt sich auf alle Inhalte anwenden, die vom selben Unternehmen an mehrere Websites geliefert werden. Wenn Sie die InPrivate-Filterung aktivieren, hindert der Internet Explorer Dritte daran, Ihre Browsersitzungen auf diese Weise über mehrere separate Websites hinweg zu verfolgen. Sie müssen die InPrivate-Filterung jedes Mal, wenn Sie eine neue Browsersitzung starten, von Hand aktivieren.

Sie konfigurieren die InPrivate-Filterung im Dialogfeld *Einstellungen der InPrivate-Filterung* (Abbildung 12.27). Sie können hier Inhalt blockieren, dem Benutzer die Auswahl erlauben, welche Inhalte blockiert oder erlaubt werden, oder die InPrivate-Filterung automatisch ausschalten. Das Dialogfeld *Einstellungen der InPrivate-Filterung* zeigt auch eine Liste der Inhaltsanbieter an, die Inhalt über mehrere Sites hinweg liefern. Sie können außerdem im Systemsteuerungsapplet *Add-Ons verwalten* Regeln für die InPrivate-Filterung importieren und exportieren.

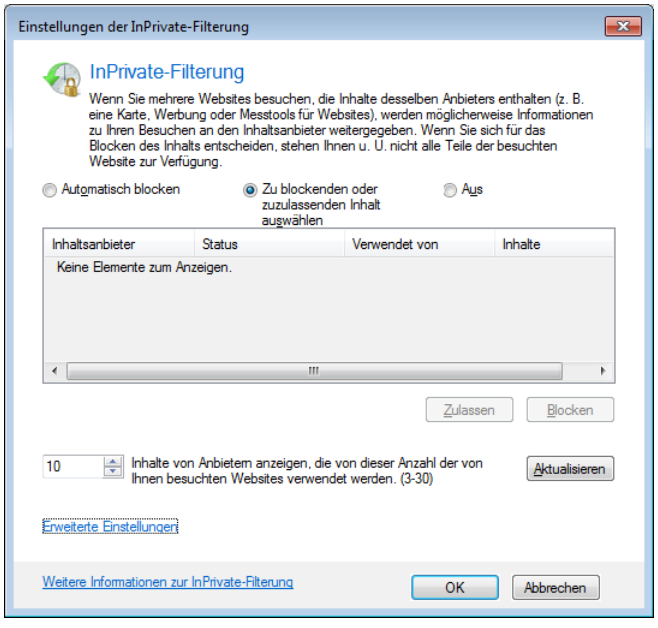

Einstellungen der InPrivate-Filterung
InPrivate-Filterung
Wenn Sie mehrere Websites besuchen, die Inhalte desselben Anbieters enthalten (z. B. eine Karte, Werbung oder Messtools für Websites), werden möglicherweise Informationen zu Ihren Besuchen an den Inhaltsanbieter weitergegeben. Wenn Sie sich für das Blocken des Inhalts entscheiden, stehen Ihnen u. U. nicht alle Teile der besuchten Website zur Verfügung.
Automatisch blocken
Zu blockenden oder zuzulassenden Inhalt auswählen
Aus
Inhaltsanbieter
Status
Verwendet von
Inhalte
Keine Elemente zum Anzeigen.
Zulassen
Blocken
10
Inhalte von Anbietern anzeigen, die von dieser Anzahl der von Ihnen besuchten Websites verwendet werden. (3-30)
Aktualisieren
Erweiterte Einstellungen
Weitere Informationen zur InPrivate-Filterung
OK
Abbrechen

Abbildung 12.27 InPrivate-Filterung

Sie können den InPrivate-Modus zentral über Gruppenrichtlinien verwalten. Diese Richtlinien befinden sich im Knoten *Administrative Vorlagen\Windows-Komponenten\Internet Explorer\InPrivate* sowohl unter *Computerkonfiguration* als auch unter *Benutzerkonfiguration*. Abbildung 12.28 zeigt die Liste dieser Richtlinien. Sie haben folgende Bedeutung:

- **InPrivate-Filterung deaktivieren** Wenn diese Richtlinie aktiviert ist, können Benutzer die InPrivate-Filterung nicht einschalten.
- **InPrivate-Browsen deaktivieren** Wenn diese Richtlinie aktiviert ist, können Benutzer das InPrivate-Browsen nicht starten.

- **Keine InPrivate-Filterungsdaten sammeln** Diese Richtlinie deaktiviert das Sammeln von Daten, das im automatischen Modus der InPrivate-Filterung durchgeführt wird.
- **Symbolleisten und Erweiterungen beim Starten des InPrivate-Browsens deaktivieren** Wenn diese Richtlinie aktiviert ist, werden zusätzliche Symbolleisten und Erweiterungen deaktiviert, sobald eine InPrivate-Browsersitzung beginnt.
- **Schwelle für InPrivate-Filterung** Der Wert, den Sie in dieser Richtlinie angeben, legt fest, wie viele vom Benutzer besuchte unterschiedliche Websites ein Element desselben Anbieters enthalten dürfen, bevor es blockiert wird. Sie können hier Werte von 3 bis 30 eintragen.

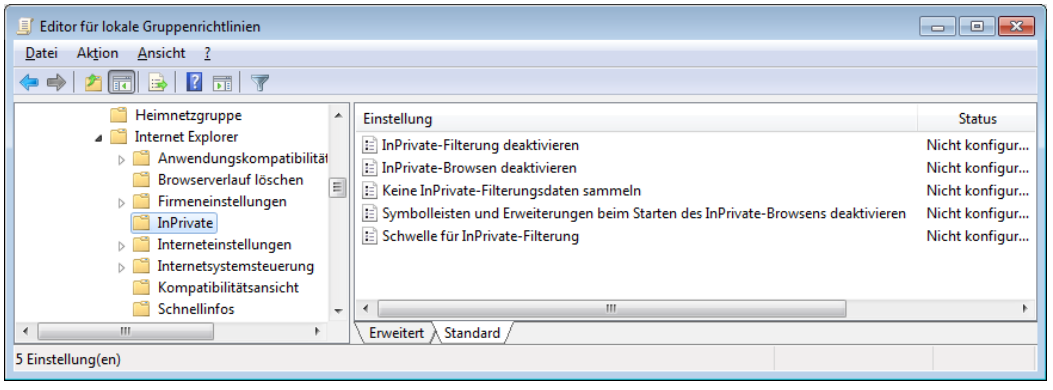


Abbildung 12.28 Richtlinien für das InPrivate-Browsen

Schnelltest

- Wie können Benutzer des Internet Explorers sicherstellen, dass keine Aufzeichnungen ihrer Browsersitzung mehr vorhanden sind, wenn sie den Browser das nächste Mal öffnen?

Antwort zum Schnelltest

- Wenn ein Benutzer den Modus *InPrivate-Browsen* aktiviert, ist sichergestellt, dass keine Aufzeichnung über eine Browsersitzung im Internet Explorer verfügbar ist.

Add-Ons und Suchanbieter

Add-Ons erweitern den Funktionsumfang des Internet Explorers. Sie werden üblicherweise einzeln heruntergeladen und installiert und nicht zusammen mit dem Internet Explorer bereitgestellt. Sie verwalten Add-Ons im Dialogfeld *Add-Ons verwalten* (Abbildung 12.29). Die Add-Ons des Internet Explorers werden in folgende Kategorien eingeteilt:

- **Symbolleisten und Erweiterungen** Dieser Bereich listet die Symbolleisten und Erweiterungen des Browsers auf. Symbolleisten sind Erweiterungen für Browser, die den Funktionsumfang der Browseroberfläche erweitern. Mithilfe von Erweiterungen kann der Browser zusätzliche Funktionen ausführen, zum Beispiel Filme abspielen oder bestimmte Dokumenttypen innerhalb des Browsers öffnen, die der Browser direkt nicht unterstützt.

- **Suchanbieter** Ermöglichen dem Benutzer, das Internet automatisch mit dem Suchfenster des Internet Explorers zu durchsuchen. Es wird ein neues Fenster oder eine neue Registerkarte geöffnet, um die Ergebnisse der Suchabfrage auf der Hauptseite des Suchmaschinenanbieters anzuzeigen.
- **Schnellinfos** Mithilfe von Schnellinfos (accelerator) können Benutzer Aktionen ausführen, nachdem sie Text ausgewählt haben. Der Internet Explorer bringt einige Standardschnellinfos mit, die Benutzer können aber selbst weitere Schnellinfos hinzufügen, indem Sie auf den Link *Weitere Schnellinfos suchen* klicken. Die Standardkategorien für Schnellinfos sind:
  - **Bloggen** Mit Schnellinfos dieser Kategorie können Sie die ausgewählten Informationen direkt in einem speziell konfigurierten Blog veröffentlichen.
  - **E-Mail** Mit Schnellinfos dieser Kategorie können Sie die ausgewählten Informationen in einer E-Mail versenden. Wenn Sie eine solche Schnellinfo öffnen, wird das E-Mail-Programm gestartet, das mit der Schnellinfo verknüpft ist. Anschließend wird der ausgewählte Text in eine neue E-Mail-Nachricht eingefügt.
  - **Karte** Mit Schnellinfos dieser Kategorie können Sie einen Onlinekartendienst nach dem Text durchsuchen, der im Browser ausgewählt ist (nur in der englischen Version).
  - **Übersetzen** Mit Schnellinfos dieser Kategorie können Sie den ausgewählten Text mit einem Onlineübersetzungsmodul in eine andere Sprache übersetzen.
- **InPrivate-Filterung** Im diesem Bereich konfigurieren Sie Elemente der InPrivate-Filterung. Sie können hier InPrivate-Filterregeln importieren und exportieren.

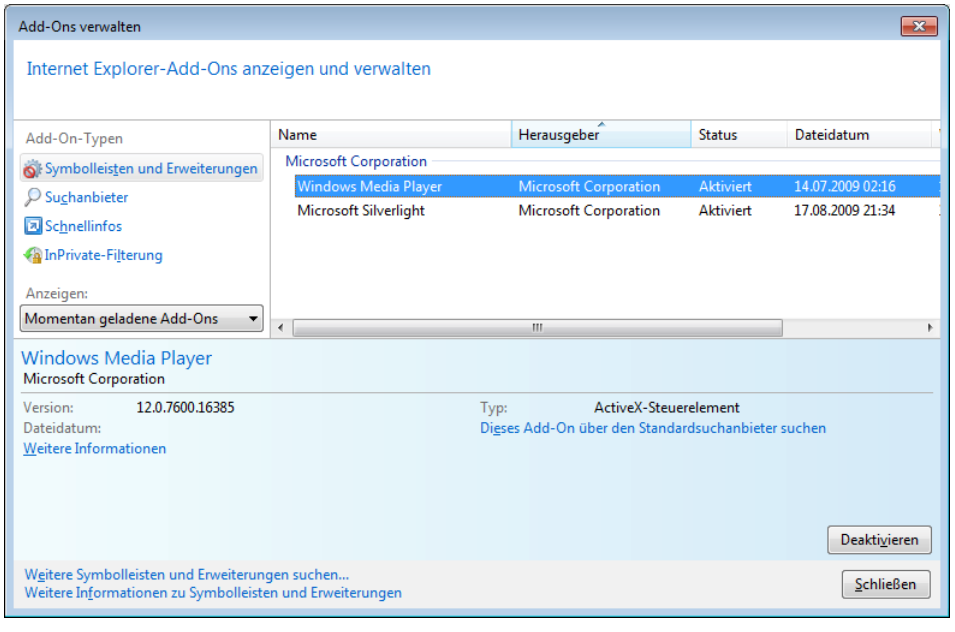


Abbildung 12.29 Verwalten der Add-Ons im Internet Explorer

Add-Ons werden normalerweise installiert, indem Sie eine Webseite besuchen, die den Add-On-Installer hostet, oder indem Sie die Software auf herkömmliche Art herunterladen und installieren. Wenn Sie eine Schnellinfo von einer Website installieren, fragt der Internet Explorer nach, ob Sie sie tatsächlich hinzufügen wollen (Abbildung 12.30). Sie sollten Add-Ons nur von Websites installieren, denen Sie vertrauen.


Schnellinfo hinzufügen
Möchten Sie diese Schnellinfo hinzufügen?
Name: "Translate with Bing"
Von: www.ieaddons.com
Ziel: www.microsofttranslator.com
Kategorie: Translate-Schnellinfo
Diesen Anbieter als Standardanbieter für diese Schnellinfokategorie festlegen
Hinzufügen
Abbrechen
Namen von Schnellinfos können irreführend sein. Fügen Sie nur Schnellinfos von Websites hinzu, denen Sie vertrauen.

Abbildung 12.30 Hinzufügen einer Schnellinfo

Sie können im Dialogfeld *Add-Ons verwalten* einzelne Add-Ons deaktivieren oder entfernen. Meist deaktivieren Sie ein Add-On, weil Probleme mit dem Internet Explorer auftreten und Sie festzustellen versuchen, ob das Add-On dafür verantwortlich ist. Sobald Sie festgestellt haben, dass ein bestimmtes Add-On die Probleme verursacht, können Sie es im Dialogfeld *Add-Ons verwalten* löschen. Windows 7 erlaubt Standardbenutzern, Add-Ons in der Standardeinstellung hinzuzufügen, zu entfernen und zu deaktivieren.

Die Richtlinien für Schnellinfos befinden sich im Knoten *Windows-Komponenten\Internet Explorer\Schnellinfos* sowohl unter *Computerkonfiguration* als auch unter *Benutzerkonfiguration*. Hier stehen folgende Gruppenrichtlinien zur Verfügung:

- **Nicht standardmäßige Schnellinfos bereitstellen** Erlaubt es, zusätzliche Schnellinfos bereitzustellen. Die Benutzer können diese Schnellinfos nicht entfernen.
- **Standardschnellinfos bereitstellen** Hier können Sie Standardschnellinfos auswählen. Die Benutzer können weitere Schnellinfos hinzufügen, aber die in dieser Richtlinie angegebenen Schnellinfos nicht ändern.
- **Schnellinfos deaktivieren** Erlaubt es, alle Schnellinfos zu deaktivieren.
- **Richtlinienschnellinfos verwenden** Diese Richtlinie schränkt die Nutzung von Schnellinfos so ein, dass nur die verwendet werden dürfen, die über die Gruppenrichtlinien verteilt werden.

Popupblocker

Der Popupblocker verhindert, dass sich Popup- und Popunder-Fenster öffnen, wenn Sie eine Seite im Internet Explorer aufrufen. Sie konfigurieren Popupblockereinstellungen, indem Sie im Internet Explorer im Menü *Extras* das Untermenü *Popupblocker* öffnen und darin den Befehl *Popupblockereinstellungen* wählen. Im Dialogfeld *Popupblockereinstellungen* können Sie die Blockierungsebene festlegen, Ausnahmen eintragen, wählen, ob eine akustisches Signal ausgegeben wird, wenn ein Popup blockiert wird, und einstellen, ob die Informations-

leiste angezeigt wird, wenn ein Popup blockiert wird. Die Standardeinstellung *Mittel* für die Blockierungsebene verhindert die meisten automatischen Popupfenster. Bei der Einstellung *Niedrig* werden nur Popups von sicheren Sites erlaubt, und bei *Hoch* werden alle Popups blockiert.

Ausnahmen sind Sites, in denen keine Popups blockiert werden. Abbildung 12.31 zeigt, wie Ausnahmen für die Sites *http://www.contoso.com* und *http://www.tailspintoys.com* eingetragen wurden. Wenn Popupinformationen in der Informationsleiste angezeigt werden dürfen, können die Benutzer ein Popupfenster bei Bedarf öffnen. Sofern Sie nicht die Einstellung *Hoch* wählen, blockiert der Internet Explorer keine Popups von Sites, die in den Sicherheitszonen *Lokales Intranet* oder *Vertrauenswürdige Sites* liegen. Die Standardeinstellungen in Windows 7 erlauben es Benutzern ohne administrative Privilegien, die Einstellungen für den Popupblocker im Systemsteuerungsapplet *Popupblockereinstellungen* zu ändern.

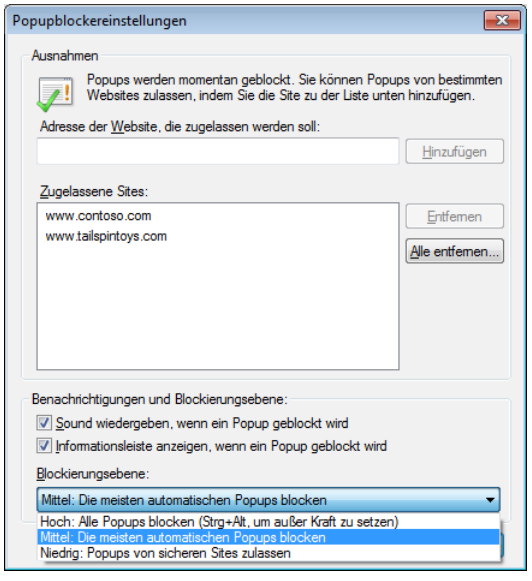

Popupblockereinstellungen
Ausnahmen
Popups werden momentan geblockt. Sie können Popups von bestimmten Websites zulassen, indem Sie die Site zu der Liste unten hinzufügen.
Adresse der Website, die zugelassen werden soll:
Hinzufügen
Zugelassene Sites:
www.contoso.com
www.tailspintoys.com
Entfernen
Alle entfernen...
Benachrichtigungen und Blockierungsebene:
Sound wiedergeben, wenn ein Popup geblockt wird
Informationsleiste anzeigen, wenn ein Popup geblockt wird
Blockierungsebene:
Mittel: Die meisten automatischen Popups blocken
Hoch: Alle Popups blocken (Strg+Alt, um außer Kraft zu setzen)
Mittel: Die meisten automatischen Popups blocken
Niedrig: Popups von sicheren Sites zulassen

Abbildung 12.31 Popupblockereinstellungen

Konfigurieren von SSL-Zertifikaten

SSL-Zertifikate stellen den Benutzern von Webbrowsern zwei nützliche Funktionen zur Verfügung. Die Benutzer können die Identität der Website überprüfen, zu der sie eine Verbindung herstellen, und es ist sichergestellt, dass die Kommunikation zwischen dem Browser und der Website mit Verschlüsselung geschützt wird.

Wenn ein Benutzer eine Site besucht, die durch ein SSL-Zertifikat geschützt ist, wird in der Adressleiste ein goldenes Schlosssymbol angezeigt, um darauf hinzuweisen. Der Benutzer kann dieses goldene Schlosssymbol anklicken, um sich Informationen über die Website anzeigen zu lassen (Abbildung 12.32). Wenn Sie im Popup *Websiteidentifizierung* auf *Zertifikate anzeigen* klicken, bekommen Sie Details zum Zertifikat aufgelistet. Das sind unter anderem die Zertifizierungsstelle, die das Zertifikat augestellt hat, das Ausstellungsdatum, die Gültigkeitsdauer des Zertifikats und die Identität der Stammzertifizierungsstelle, die am

Anfang der Zertifizierungskette steht. Wenn Sie auf *Ist diese Site vertrauenswürdig?* klicken, bekommen Sie Informationen dazu, ob Sie der Website vertrauen können.

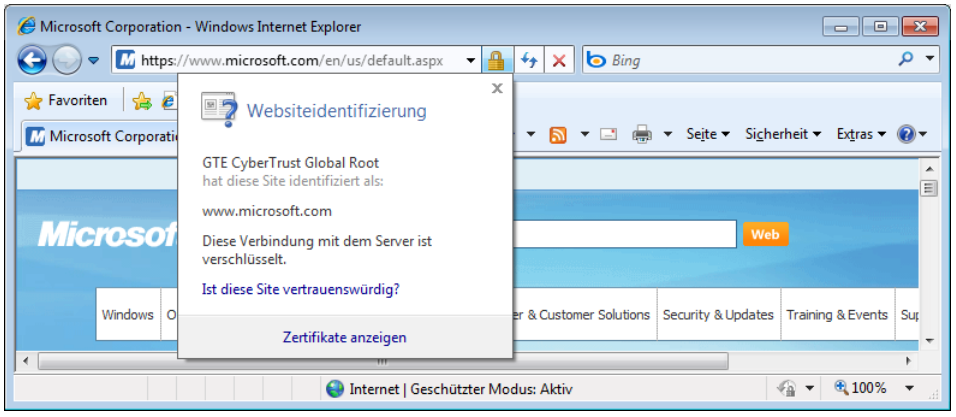


Abbildung 12.32 Informationen zu einer sicheren Website

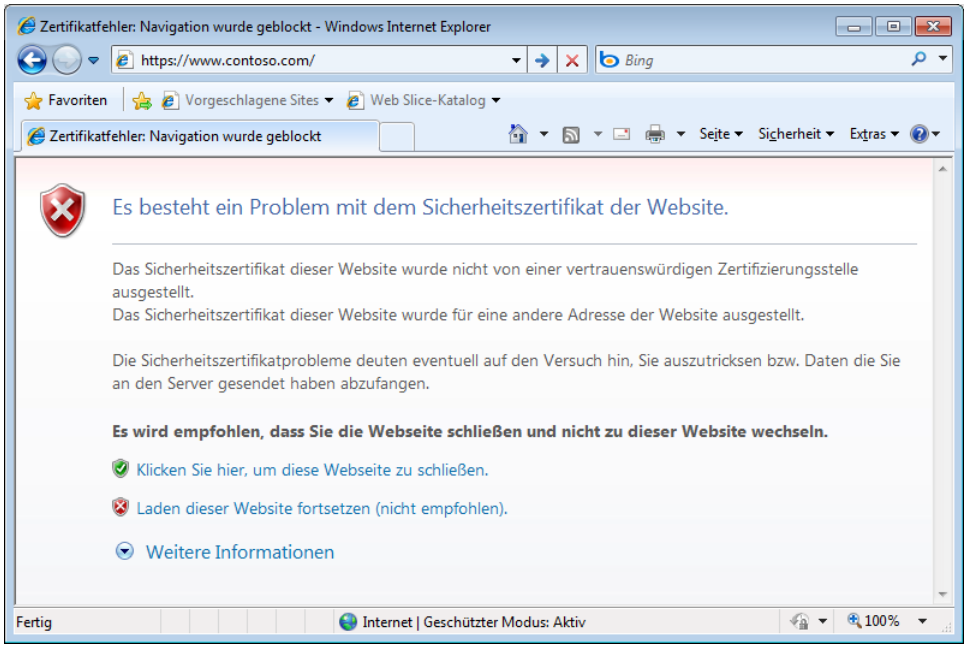

Zertifikatfehler: Navigation wurde geblockt - Windows Internet Explorer
https://www.contoso.com/
Bing
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Zertifikatfehler: Navigation wurde geblockt
Seite
Sicherheit
Extras
Es besteht ein Problem mit dem Sicherheitszertifikat der Website.
Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.
Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt.
Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.
Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.
Klicken Sie hier, um diese Webseite zu schließen.
Laden dieser Website fortsetzen (nicht empfohlen).
Weitere Informationen
Fertig
Internet | Geschützter Modus: Aktiv
100%

Abbildung 12.33 Problem mit einem Websitezertifikat

Der Internet Explorer zeigt eine Warnung an, wenn Sie eine geschützte Website besuchen, bei der ein Problem mit dem SSL-Zertifikat besteht. Im Beispiel aus Abbildung 12.33 lautet der Name, der auf dem Zertifikat der Website *https://www.contoso.com* benutzt wird, nicht *www.contoso.com*. Der Internet Explorer blockiert die Navigation auf diese Website automatisch. Ein Benutzer muss auf *Laden dieser Website fortsetzen (nicht empfohlen)* klicken, um zur Website zu navigieren. Dieses Problem kann auftreten, wenn eine Website vor Kurzem ihren Namen geändert hat, aber noch das Zertifikat benutzt, in dem der bisherige Name

steht. Es kann aber auch sein, dass die Domäne gekidnappt wurde oder ein anderes Problem mit der Site besteht, das die Sicherheit gefährdet. Sie sollten Benutzer ermahnen, vorsichtig zu sein, wenn dieser Fehler auftaucht. Auf keinen Fall sollten sie vertrauliche Daten in einer Website eingeben, bei der SSL-Zertifikat und Websitename nicht übereinstimmen. Ohne einwandfreies Zertifikat ist es nämlich nicht möglich, die Identität der Website zu überprüfen. Selbst wenn eine Site seriös ist, sollten Sie es sich noch einmal überlegen, ob Sie vertrauliche Daten über das Internet an ein Unternehmen übermitteln, das nicht in der Lage ist, sein SSL-Zertifikat auf dem neusten Stand zu halten.

Der Internet Explorer blockiert die Navigation auf eine Website, wenn die Anwendung folgende Arten von Zertifikatfehlern erkennt:

- **Websiteadresse stimmt nicht mit der Adresse im Zertifikat überein** Dieser Fehler tritt auf, wenn eine Website ein digitales Zertifikat benutzt, das für eine andere Webadresse ausgestellt wurde. Das passiert oft, wenn eine Organisation mehrere Websites auf demselben Server hostet.
- **Websitezertifikat wurde gesperrt** Dieser Fehler macht darauf aufmerksam, dass das Sicherheitszertifikat mit betrügerischen Mitteln von der Website ausgespäht oder benutzt wurde. Die Organisation, die das Zertifikat ausgestellt hat, hat das Zertifikat gesperrt. Das bedeutet, dass Sie der Website nicht mehr vertrauen sollten.
- **Websitezertifikat ist nicht mehr gültig** Dieser Fehler tritt auf, wenn das aktuelle Datum außerhalb des Gültigkeitszeitraums des Zertifikats liegt (also davor oder danach). Beispielsweise erhalten Sie diesen Fehler bei einem Zertifikat, das von 2100 bis 2150 gültig ist, aber genauso bei einem Zertifikat, das von 1996 bis 2000 gültig war. Websites müssen Zertifikate regelmäßig bei den Zertifizierungsstellen erneuern.
- **Websitezertifikat stammt nicht aus einer vertrauenswürdigen Quelle** Dieser Fehler bedeutet, dass das Websitezertifikat von einer Zertifizierungsstelle ausgestellt wurde, der der Internet Explorer nicht vertraut. Das ist oft bei Webservern in Intranetsites der Fall. Wenn Sie diesen Fehler beim Aufrufen einer Internetsite erhalten, sollten Sie ihr nicht vertrauen, weil viele Phishingsites Identitätszertifikate fälschen, um zu versuchen, die Benutzer von ihrer Echtheit zu überzeugen. Wie Sie den Internet Explorer so konfigurieren, dass er seriösen Quellen vertraut, wird weiter unten in dieser Lektion genauer beschrieben.
- **Problem mit dem Sicherheitszertifikat** Dieser Fehler tritt auf, wenn der Internet Explorer ein Problem mit einem Websitezertifikat erkennt, das nicht in die anderen Kategorien fällt. Sie bekommen diesen Fehler, wenn jemand das Zertifikat manipuliert hat oder es beschädigt wurde. Sie sollten Websites nicht vertrauen, bei deren Sicherheitszertifikat der Internet Explorer ein Problem meldet.

Wenn Sie geschützte Sites in nichtöffentlichen Netzwerken wie einem Unternehmensintranet besuchen, bekommen Sie es möglicherweise mit Websitezertifikaten zu tun, die von einer Zertifizierungsstelle ausgestellt wurden, der der Internet Explorer nicht vertraut. Das passiert oft, weil Organisationen eine interne PKI (Public Key Infrastructure) einrichten, um Zertifikate an interne Hosts zu verteilen. Sie brauchen dabei kein öffentlich überprüftes SSL-Zertifikat, um einen internen Server zu identifizieren. In den meisten Organisationen, die eine eigene PKI aufbauen, vertrauen die Clients automatisch den ausstellenden Zertifizierungsstellen, weil es möglich ist, ihre Zertifikate über AD DS zu veröffentlichen. Sie können den Internet Explorer so konfigurieren, dass er einer Zertifizierungsstelle vertraut, indem Sie die Website der Zertifizierungsstelle aufrufen, ihr Zertifikat abrufen und es installieren.

Die aktuelle Liste der Zertifikate können Sie sich auf der Seite *Inhalte* im Dialogfeld *Internetoptionen* ansehen (Abbildung 12.34). Sie können die momentan zwischengespeicherten SSL-Zertifikate löschen, indem Sie auf *SSL-Status löschen* klicken. Die aktuellen Zertifikate können Sie sich ansehen, indem Sie auf *Zertifikate* klicken. Und wenn Sie auf *Herausgeber* klicken, bekommen Sie die vertrauenswürdigen Zertifizierungsstellen aufgelistet. Mit den Schaltflächen *Zertifikate* und *Herausgeber* können Sie Zertifikate importieren oder exportieren. Wenn Sie beispielsweise eine E-Mail erhalten haben, die das Zertifikat der internen Zertifizierungsstelle Ihres Unternehmens enthält, können Sie den Internet Explorer so konfigurieren, dass er dieser Zertifizierungsstelle vertraut, indem Sie das Zertifikat in diesem Dialogfeld importieren.

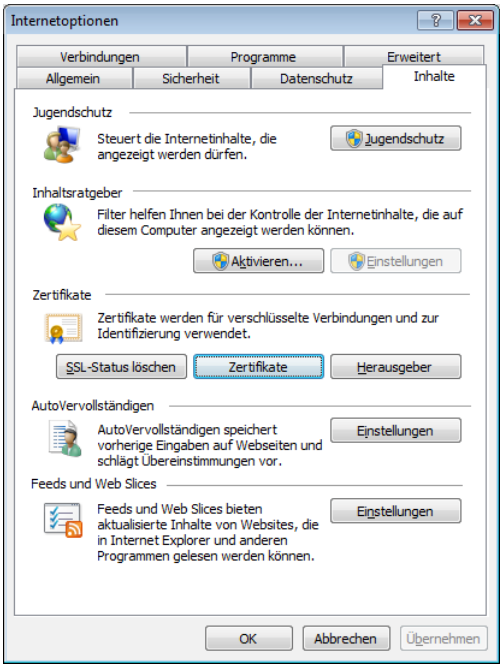


Abbildung 12.34 Verwalten von Zertifikaten



Prüfungstipp

Machen Sie sich damit vertraut, worin sich die Funktionen von InPrivate-Browsen und InPrivate-Filterung unterscheiden.

Übung InPrivate-Modus und Add-Ons

In dieser Übung untersuchen Sie, wie das InPrivate-Browsen funktioniert, und verwalten Add-Ons im Internet Explorer. InPrivate-Browsen ist ein Feature, an dem viele Leute interessiert sind, die sich ihren Computer mit anderen Personen teilen. Auf diese Weise können sie ihre Webbrowsingaktivitäten vor den anderen Leuten verborgen halten, die den Computer ebenfalls benutzen. Der Computer *Canberra* muss Zugriff auf das Internet haben, damit Sie die beiden folgenden Übungen durcharbeiten können.

Übung 1 Ausprobieren des InPrivate-Modus

In dieser Übung machen Sie sich mit dem InPrivate-Modus von Internet Explorer 8 vertraut. Beim InPrivate-Modus werden keine Daten über eine Browsersitzung gespeichert. In dieser Übung verwenden Sie den Browser im normalen Modus, dann im InPrivate-Modus. Anschließend untersuchen Sie, wo die Unterschiede liegen. Gehen Sie folgendermaßen vor.

1. Melden Sie sich unter dem Benutzerkonto *Kim_Akers* am Computer *Canberra* an.
2. Öffnen Sie den Internet Explorer über die Taskleiste. Wenn sich der Assistent *Willkommen zu Internet Explorer 8* öffnet, können Sie auf *Später erneut nachfragen* klicken.
3. Stellen Sie sicher, dass nur eine Registerkarte offen ist. Geben Sie in der Adressleiste die Adresse **http://www.bing.com** ein und drücken Sie die EINGABETASTE.
4. Geben Sie im Textfeld der Suchmaschine **70-680 site:microsoft.com** ein und klicken Sie auf die Suchschaltfläche. Das Ergebnis sollte ähnlich wie in Abbildung 12.35 aussehen.

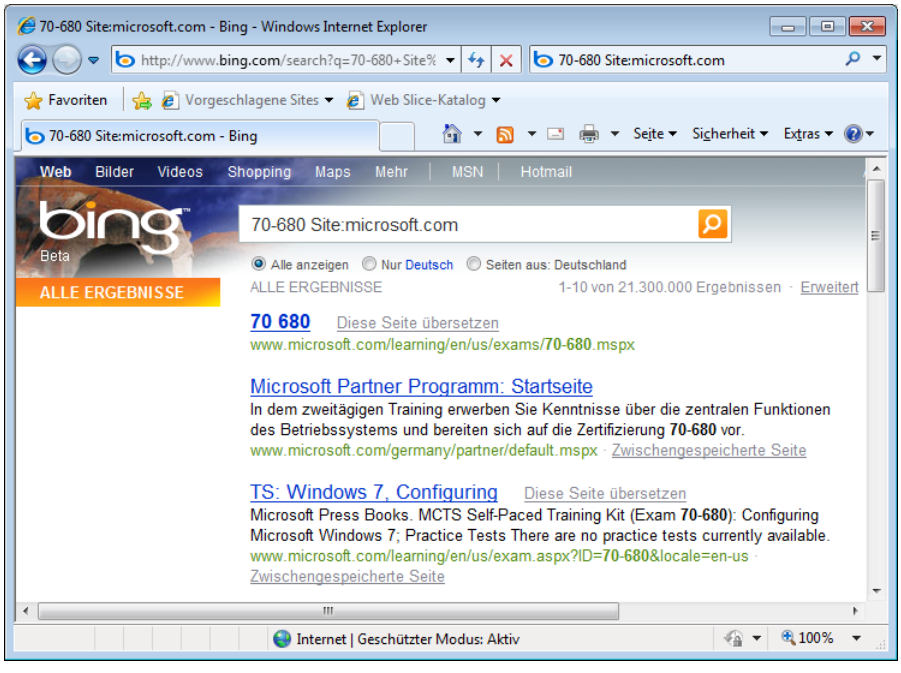


Abbildung 12.35 Ergebnisse der Suche nach 70-680

5. Klicken Sie auf den Link *TS: Windows 7, Configuring*. Damit gelangen Sie auf die englische Webseite für die Prüfung 70-680. Klicken Sie auf der rechten Seite unter *Related Services* auf *E-Reference Libraries*. Daraufhin öffnet sich die Seite *E-Reference Libraries*.
6. Klicken Sie im Menü *Sicherheit* auf *Browserverlauf löschen*. Aktivieren Sie im Dialogfeld *Browserverlauf löschen* alle Kontrollkästchen, wie in Abbildung 12.36 gezeigt, und klicken Sie auf *Löschen*.

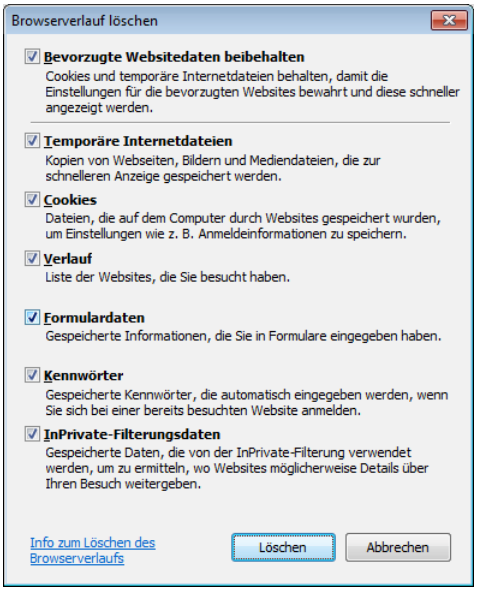

Browserverlauf löschen
Bevorzugte Websitedaten beibehalten
Cookies und temporäre Internetdateien behalten, damit die Einstellungen für die bevorzugten Websites bewahrt und diese schneller angezeigt werden.
Temporäre Internetdateien
Kopien von Webseiten, Bildern und Mediendateien, die zur schnelleren Anzeige gespeichert werden.
Cookies
Dateien, die auf dem Computer durch Websites gespeichert wurden, um Einstellungen wie z. B. Anmeldeinformationen zu speichern.
Verlauf
Liste der Websites, die Sie besucht haben.
Formulardaten
Gespeicherte Informationen, die Sie in Formulare eingegeben haben.
Kennwörter
Gespeicherte Kennwörter, die automatisch eingegeben werden, wenn Sie sich bei einer bereits besuchten Website anmelden.
InPrivate-Filterungsdaten
Gespeicherte Daten, die von der InPrivate-Filterung verwendet werden, um zu ermitteln, wo Websites möglicherweise Details über Ihren Besuch weitergeben.
Info zum Löschen des Browserverlaufs
Löschen
Abbrechen

Abbildung 12.36 Dialogfeld *Browserverlauf löschen*

7. Schließen Sie den Internet Explorer, sobald der Browserverlauf gelöscht wurde.
8. Öffnen Sie den Internet Explorer erneut. Wählen Sie im Menü *Extras* den Befehl *Letzte Browsersitzung erneut öffnen*. Daraufhin öffnet sich die letzte Seite, die Sie in der vorherigen Sitzung besucht haben. Und das, obwohl Sie den Browserverlauf gelöscht haben.
9. Klicken Sie auf das Pfeilsymbol links neben der Adressleiste. Wie sie sehen, sind alle Seiten, die Sie in der vorherigen Sitzung besucht haben, darunter der Inhalt der Suchergebnisse auf *bing.com*, in der neu geöffneten Browsersitzung gespeichert (Abbildung 12.37).

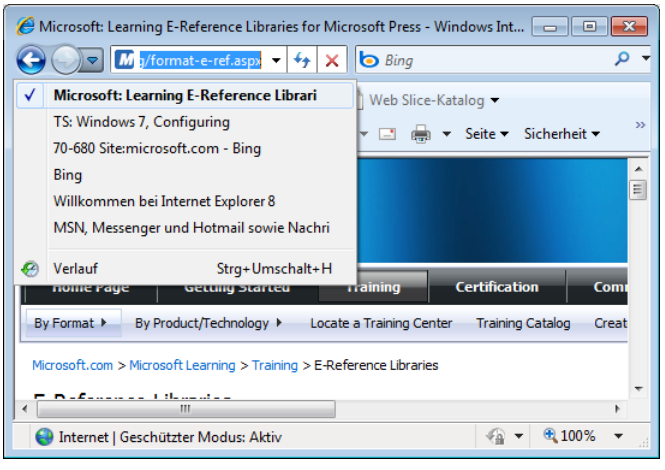


Abbildung 12.37 Die Daten der letzten Sitzung sind immer noch vorhanden

10. Schließen Sie den Internet Explorer.
11. Öffnen Sie den Internet Explorer erneut. Wählen Sie im Menü *Sicherheit* den Befehl *InPrivate-Browsen*. Daraufhin öffnet sich das Fenster für das InPrivate-Browsen.
12. Geben Sie in der Adressleiste des InPrivate-Browserfensters die Adresse **http://www.bing.com** ein und drücken Sie die EINGABETASTE.
13. Geben Sie im Textfeld **Windows 7 site:microsoft.com** ein und drücken Sie die EINGABETASTE.
14. Klicken Sie in den Suchergebnissen auf den Link *Windows 7 Startseite*, dem die URL (Uniform Resource Locator) *www.microsoft.com/germany/windows/windows-7* zugeordnet ist. Daraufhin wird die deutschsprachige Startseite zu Windows 7 geöffnet.
15. Schließen Sie alle offenen Internet Explorer-Fenster.
16. Öffnen Sie den Internet Explorer erneut. Wählen Sie im Menü *Extras* den Befehl *Letzte Browsersitzung erneut öffnen*. Wie Sie sehen, sind diesmal keine der Seiten vorhanden, auf denen Sie in der vorherigen Sitzung nach Informationen über Windows 7 gesucht haben, weder im Browserverlauf noch innerhalb der vorherigen Sitzung.
17. Schließen Sie den Internet Explorer.

Übung 2 Verwalten von Add-Ons für Internet Explorer

In dieser Übung konfigurieren und verwalten Sie Add-Ons für den Internet Explorer. Gehen Sie folgendermaßen vor:

1. Melden Sie sich unter dem Benutzerkonto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Öffnen Sie den Internet Explorer. Wählen Sie im Menü *Extras* den Befehl *Add-Ons verwalten*. Daraufhin öffnet sich das Dialogfeld *Add-Ons verwalten*.
3. Wählen Sie den Eintrag *Suchanbieter* aus und klicken Sie auf den Link *Weitere Suchanbieter suchen*. Der Internet Explorer ruft nun eine Webseite auf, die eine Add-On-Galerie enthält. Wählen Sie in der Add-On-Galerie einen Suchanbieter aus und klicken Sie auf *Dem Internet Explorer hinzufügen*. Klicken Sie im Dialogfeld *Suchanbieter hinzufügen* (Abbildung 12.38) auf *Hinzufügen*.

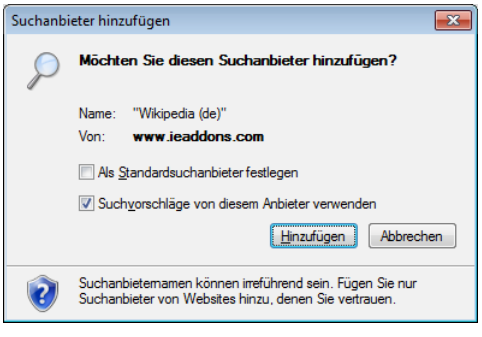

Suchanbieter hinzufügen
Möchten Sie diesen Suchanbieter hinzufügen?
Name: "Wikipedia (de)"
Von: www.ieaddons.com
Als Standardsuchanbieter festlegen
Suchvorschläge von diesem Anbieter verwenden
Hinzufügen
Abbrechen
Suchanbietemamen können irreführend sein. Fügen Sie nur Suchanbieter von Websites hinzu, denen Sie vertrauen.

Abbildung 12.38 Hinzufügen eines Suchanbieters

4. Schließen Sie das Dialogfeld *Add-Ons verwalten* und öffnen Sie es erneut. Wie Sie sehen, wird nun der Suchanbieter aufgelistet, den Sie eben installiert haben. Wählen

Sie den Eintrag *Schnellinfos* aus und klicken Sie auf *Weitere Schnellinfos suchen*. Der Internet Explorer ruft wieder die Webseite mit der Add-On-Galerie auf. Diesmal werden Schnellinfos aufgelistet. Klicken Sie auf die Kategorie *Andere*. Suchen Sie die Schnellinfo *MSDN* (Abbildung 12.39) und klicken Sie auf *Dem Internet Explorer hinzufügen*.

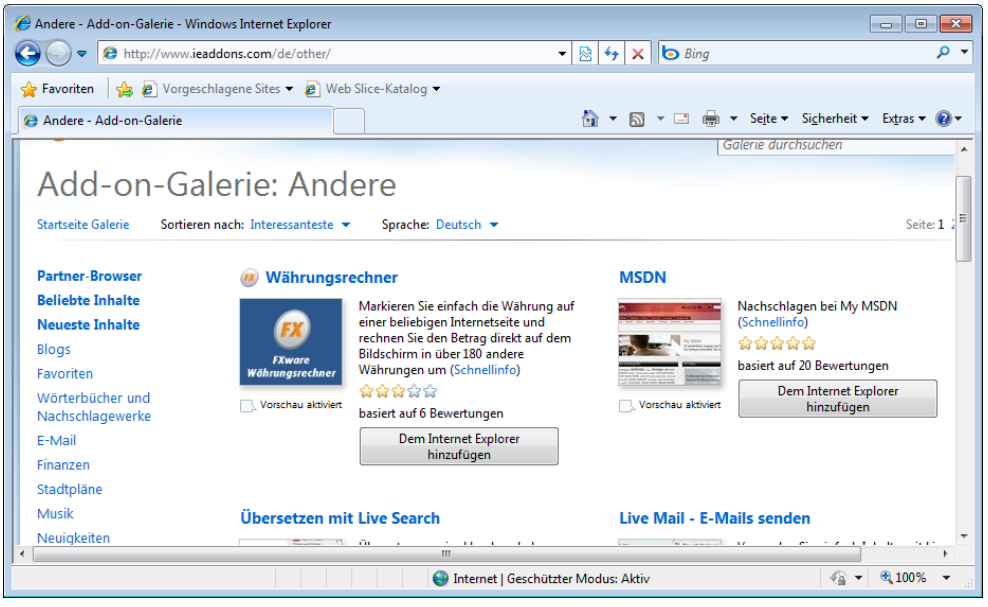


Abbildung 12.39 Auswählen einer Schnellinfo

5. Klicken Sie im Dialogfeld *Möchten Sie diese Schnellinfo hinzufügen?* auf *Hinzufügen*. Schließen Sie das Dialogfeld *Add-Ons verwalten* und öffnen Sie es erneut. Prüfen Sie, ob die ausgewählte Schnellinfo nun aufgelistet wird.
6. Wählen Sie die neu installierte Schnellinfo *Nachschlagen bei My MSDN* aus und klicken Sie auf *Als Standard*. Klicken Sie auf *Schließen*, um das Dialogfeld *Add-Ons verwalten* zu schließen.
7. Rufen Sie im Internet Explorer die folgende URL auf: *http://www.microsoft.com/germany/windows/windows-7/*
8. Wählen Sie den Textabschnitt mit dem Begriff »Windows 7 Upgrade Advisor« aus.
9. Klicken Sie auf das Schnellinfosymbol und dann auf die Schnellinfo *Nachschlagen bei My MSDN*, die Sie installiert haben. Der Internet Explorer zeigt nun die MSDN-Seite an, auf der Links zum Tool Windows 7 Upgrade Advisor aufgelistet sind.
10. Klicken Sie im Menü *Extras* auf *Add-Ons verwalten*. Wählen Sie den Eintrag *Schnellinfos* aus und klicken Sie auf die *MSDN*-Schnellinfo, die Sie installiert haben. Klicken Sie auf *Deaktivieren*, um diese Schnellinfo zu deaktivieren. Klicken Sie auf *Schließen*, um das Dialogfeld *Add-Ons verwalten* zu schließen.
11. Schließen Sie den Internet Explorer.

Zusammenfassung der Lektion

- Die Kompatibilitätsansicht ermöglicht es, Seiten, die in Internet Explorer 8 nicht richtig angezeigt werden, aber in Internet Explorer 7 funktionieren, auch in Internet Explorer 8 richtig darzustellen. Sie können die Kompatibilitätsansicht von Hand konfigurieren, eine Liste von Websites verwenden, die Microsoft zur Verfügung stellt und über Windows Update aktualisiert, oder von Hand eine Liste der Sites zusammenstellen, die der Internet Explorer in der Kompatibilitätsansicht darstellen soll.
- Sicherheitseinstellungen konfigurieren Sie in erster Linie, indem Sie Sites an Zonen zuweisen. Sites, die höhere Privilegien erfordern, sollten der Zone *Vertrauenswürdige Sites* zugewiesen werden. Sites, die im Intranet liegen, werden automatisch der Zone *Lokales Intranet* zugewiesen; allerdings setzt das in bestimmten Fällen eine manuelle Konfiguration voraus. Alle anderen Sites werden der Zone *Internet* zugewiesen. Die Zone *Eingeschränkte Sites* wird nur für Websites benutzt, die möglicherweise die Sicherheit gefährden, aber besucht werden müssen.
- Add-Ons erweitern den Funktionsumfang des Internet Explorers. Benutzer mit Standardberechtigungen können Add-Ons hinzufügen, entfernen und deaktivieren, sofern das nicht von Gruppenrichtlinien verhindert wird. Mit Schnellinfos können Benutzer Text auf einer Webseite markieren und dann automatisch eine andere Funktion ausführen, den Text beispielsweise übersetzen oder an ein Blog weiterleiten. Weitere Suchanbieter können problemlos zum Suchfenster hinzugefügt werden.
- InPrivate-Browsen verhindert, dass der Internet Explorer Daten über eine Browsersitzung speichert. Die InPrivate-Filterung hindert fremde Websites daran, Daten über Sie zu sammeln, während Sie mehrere Sites besuchen.
- Der Internet Explorer zeigt Benachrichtigungen an, wenn die Adresse einer Website nicht mit dem SSL-Zertifikat übereinstimmt, das sie dem Client übergibt, oder wenn das Zertifikat abgelaufen, gesperrt oder beschädigt ist.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Konfigurieren von Internet Explorer«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie arbeiten mehrere Wochen als Consultant bei Contoso. Sie versuchen, im Internet Explorer eine Verbindung zu einer Webanwendung herzustellen, die unter *https://timesheet.contoso.internal* eine Stundenabrechnung zur Verfügung stellt. Sie bekommen die Meldung, dass das Websitezertifikat nicht von einer vertrauenswürdigen Quelle ausgestellt wurde. Wie können Sie dieses Problem beseitigen?
   A. Konfigurieren Sie die Sicherheitsstufe der Zone *Intranet*.
   B. Schalten Sie den Popupblocker aus.

C. Starten Sie das InPrivate-Browsen und rufen Sie die Website erneut auf.

D. Rufen Sie die Zertifizierungsstelle *contoso.internal* im Internet Explorer auf und installieren Sie das Zertifikat der Zertifizierungsstelle.

2. Entwickler in Ihrer Organisation haben ein eigenes Bloggingtool und eine Schnellinfo entwickelt, die es ermöglichen, Blogs direkt im Unternehmensintranet zu veröffentlichen. Sie möchten den Benutzern die Möglichkeit bieten, interessante Textstellen, die sie auf Webseiten finden, zu markieren und direkt in einem Blog zu veröffentlichen, das auf dem Intranetserver gehostet wird. Sie wollen sicherstellen, dass die Benutzer ihre Texte nicht versehentlich mit der Standardschnellinfo *Mit Windows Live bloggen* veröffentlichen. Wie sollten Sie auf jedem Computer vorgehen, um dieses Ziel zu erreichen? (Wählen Sie alle zutreffenden Antworten aus; sie bilden zusammen die richtige Lösung.)

   A. Deaktivieren Sie die Schnellinfo *Mit Windows Live bloggen*.

   B. Installieren Sie die selbstentwickelte Blog-Schnellinfo.

   C. Machen Sie die Schnellinfo *Mit Windows Live bloggen* zur Standardblogschnellinfo für den Internet Explorer.

   D. Deaktivieren Sie die selbstentwickelte Blogschnellinfo.

3. Sie wollen sicherstellen, dass der Internet Explorer außer auf der Site *http://www.wingtiptoys.com* keine Popupfenster öffnet. Welche der folgenden Einstellungen sollten Sie im Dialogfeld *Popupblockereinstellungen* konfigurieren? (Wählen Sie alle zutreffenden Antworten aus; sie bilden zusammen die richtige Lösung.)

   A. Tragen Sie *http://www.wingtiptoys.com* als Ausnahme ein.

   B. Setzen Sie die Blockierungsebene auf *Mittel*.

   C. Setzen Sie die Blockierungsebene auf *Hoch*.

   D. Setzen Sie die Blockierungsebene auf *Niedrig*.

4. Ihr Unternehmen hat vor Kurzem mehrere kleinere Firmen aufgekauft. Alle diese Tochterfirmen haben eine eigene Internetsite, und jede dieser Sites hat einen eindeutigen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN). Alle Clients benutzen Windows 7 Enterprise mit den Standardeinstellungen. Mehrere Intranetwebsites der Tochterfirmen werden im Internet Explorer unter Windows 7 nicht richtig dargestellt. In Clients, die unter Windows XP und Windows Vista laufen, zeigt der Internet Explorer diese Seite einwandfrei an. Alle Clients, die unter Windows 7 laufen, sind Mitglieder derselben AD DS-Domäne. Welche der folgenden Konfigurationsänderungen sollten Sie an den Gruppenrichtlinien vornehmen, um dieses Problem zu lösen?

   A. Aktivieren Sie die Richtlinie *InPrivate-Browsen deaktivieren*.

   B. Aktivieren Sie die Richtlinie *InPrivate-Filterung deaktivieren*.

   C. Aktivieren Sie die Richtlinie *Kompatibilitätsansicht deaktivieren*.

   D. Konfigurieren Sie die Richtlinie *Richtlinienliste von Internet Explorer 7-Sites verwenden*.

5. Sie wollen sicherstellen, dass Websites von Herstellern, die Inhalt für mehrere andere Sites zuliefern, nicht verfolgen können, welche Sites Sie während einer Browsersitzung besuchen. Welche der folgende Einstellungen sollten Sie nach dem Starten des Internet Explorers vornehmen, um sicherzustellen, dass dies nicht geschieht?
   A. Starten Sie eine Sitzung mit *InPrivate-Browsen*
   B. Aktivieren Sie die InPrivate-Filterung
   C. Deaktivieren Sie den Popupblocker
   D. Deaktivieren Sie den SmartScreen-Filter

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Windows Update ist ein in Windows 7 eingebautes Feature, das verwaltet, wie Softwareupdates heruntergeladen und installiert werden.
- Windows Update kann Updates von den Microsoft Update-Servern im Internet oder aus einer lokalen Updatequelle abrufen, beispielsweise einem WSUS-Server.
- Manche Windows Update-Server können über das Windows Update-Systemsteuerungsapplet konfiguriert werden, aber die meisten Einstellungen werden über Gruppenrichtlinien vorgenommen.
- Beim InPrivate-Browsen zeichnet der Internet Explorer keine Daten zur Browsersitzung auf.
- Add-Ons des Internet Explorers erweitern den Funktionsumfang des Browsers.
- Sicherheitszonen ermöglichen es, Websites nach ihrer Vertrauenswürdigkeit einzustufen.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **InPrivate-Browsen**
- **InPrivate-Filterung**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie an, was Sie zu den Themen dieses Kapitels gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Windows Update bei Contoso

Contoso hat drei Niederlassungen in Australien. Die Hauptstelle liegt in Canberra, außerdem gibt es Zweigstellen in Adelaide und Brisbane. Alle Clientcomputer bei Contoso laufen unter Windows 7 Enterprise. Sie sind so konfiguriert, dass Sie sich über das Netzwerk mithilfe einer Remotedesktopverbindung anmelden können. Es stehen Energiesparfeatures zur Verfügung, die es ermöglichen, die Clientcomputer aus dem Ruhezustand aufzuwecken. Sie haben gerade die WSUS-Rolle im Büro Canberra installiert. Sie wollen, dass die Computer in der Niederlassung Canberra den WSUS-Server für ihre Updates benutzen, die Computer in Adelaide und Brisbane Ihre Updates aber von Microsoft Update abrufen. Ein anderes Problem hat mit einer Anwendung zu tun, die auf Computern in den Niederlassungen Adelaide und Brisbane installiert ist. Sie haben gerade vom Softwarehersteller erfahren, dass ein kürzliches Update, das in KB123456 beschrieben ist, dazu führt, dass die Anwendung nicht mehr richtig funktioniert.

Beantworten Sie folgende Fragen:

1. Welche Richtlinie sollten Sie für die Computer in der Niederlassung Canberra konfigurieren, um sicherzustellen, dass sie den lokalen WSUS-Server verwenden und nicht die Microsoft Update-Server im Internet?
2. Welche Richtlinie sollten Sie konfigurieren, um sicherzustellen, dass Computer für die Installation von Softwareupdates aus dem Ruhezustand aufgeweckt werden?
3. Wie sollten Sie das Update KB123456 von den Computern in den Niederlassungen Brisbane und Adelaide entfernen und wie können Sie sicherstellen, dass es nicht installiert wird, bis das Problem mit der Anwendung beseitigt ist?

Übung mit Fallbeispiel 2: Internet Explorer bei Wingtip Toys

Sie haben vor Kurzem die Bereitstellung von 100 Computern mit Windows 7 Enterprise bei WingTip Toys geleitet. WingTip Toys und seine Tochterfirma Tailspin Toys verkaufen leistungsfähige ferngesteuerte Modellflugzeuge. Im Rahmen der Windows 7-Bereitstellung müssen Sie sich um folgende Probleme kümmern, die nach der Migration aufgetreten sind:

- Einige Mitarbeiter der Forschungsabteilung machen sich Sorgen, dass ihre Webbrowsersitzungen von Konkurrenten über mehrere Websites hinweg verfolgt werden könnten. Dieses Problem ist zwar schon seit einiger Zeit bekannt, aber einige Mitarbeiter haben gelesen, dass Windows 7 spezielle Techniken enthält, die solche Probleme vermeiden sollen.
- Nach mehreren Vorfällen, bei denen Unternehmensdaten versehentlich in externen Blogs veröffentlicht wurden, möchten Sie die Verwendung von Schnellinfos in Internet Explorer 8 möglichst weit einschränken.
- Das Unternehmen unterhält zwei externe Websites: *http://www.tailspintoys.com* und *http://www.wingtiptoys.com*. Diese Websites werden im Internet Explorer 8 nicht sauber dargestellt. Im Internet Explorer 7 auf Clients, die unter Windows XP und Windows

Vista laufen, sehen sie dagegen einwandfrei aus. Das Unternehmen hat vor, die Sites zu überarbeiten, aber es wurde noch kein konkreter Zeitplan dafür aufgestellt.

Beantworten Sie folgende Fragen:

1. Wie stellen Sie sicher, dass die Benutzer überhaupt keine Schnellinfos im Internet Explorer verwenden können?
2. Wie können die Mitarbeiter der Forschungsabteilung sicherstellen, dass ihre Browsersitzungen nicht über mehrere Websites hinweg verfolgt werden?
3. Wie stellen Sie sicher, dass die Sites *http://www.tailspintoys.com* und *http://www.wingtiptoys.com* von Clients bei WingTip Toys immer in der Kompatibilitätsansicht angezeigt werden?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Konfigurieren von Updates für Windows 7

Diese Übungen können Sie nur vollständig durcharbeiten, wenn Sie mit dem Internet verbunden sind.

- **Übung 1** Führen Sie Windows Update aus, prüfen Sie, ob Updates verfügbar sind, und installieren Sie alle Updates, die als wichtig oder empfohlen markiert sind. Starten Sie den Computer neu, sofern nötig.
- **Übung 2** Deinstallieren Sie eines der Updates, sobald Sie alle verfügbaren Updates installiert haben, sodass keine weiteren Updates mehr anstehen. Prüfen Sie im Systemsteuerungsapplet *Windows Update* erneut, ob Updates verfügbar sind. Nun müsste das Update, das Sie deinstalliert haben, erneut zur Installation angeboten werden. Blenden Sie dieses Update mit dem Systemsteuerungsapplet *Windows Update* aus. Prüfen Sie wiederum mit Windows Update, ob Updates verfügbar sind. Nun dürften keine wichtigen oder empfohlenen Updates mehr aufgeführt sein. Stellen Sie das ausgeblendete Update wieder her. Prüfen Sie erneut mit Windows Update, ob Updates verfügbar sind. Installieren Sie das Update wieder.

Konfigurieren von Internet Explorer

Diese Übungen können Sie nur vollständig durcharbeiten, wenn Sie mit dem Internet verbunden sind.

- **Übung 1** Fügen Sie Schnellinfos für die Kategorien Bloggen, E-Mail und Übersetzen zum Internet Explorer hinzu.
- **Übung 2** Öffnen Sie die Registerkarte *Sicherheit* des Dialogfelds *Internetoptionen*. Klicken Sie auf die Schaltfläche *Stufe anpassen* und sehen Sie sich die einzelnen Einstellungen für jede Zone an. Stellen Sie fest, welche Zonen dem Benutzer erlauben, signierte und unsignierte ActiveX-Steuerelemente herunterzuladen.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

K A P I T E L 1 3

Überwachung und Leistung

Dieses Kapitel beschäftigt sich mit der Überwachung der Ressourcen und der Leistung auf einem Windows 7-Computer. Es stellt die verschiedenen Tools vor, die Ihnen verraten, welche Ressourcen auf einem Computer verfügbar sind und Probleme bei der Ressourcenauslastung melden. Das Kapitel beschreibt die Leistungsüberwachung und erklärt, wie Sie Baselines (Referenzwerte) messen, Protokolle anlegen und potenzielle Leistungsengpässe aufdecken, bevor sie zum Problem werden. Sie erfahren, wie Sie ermitteln, ob Computer in der Lage sind, ressourcenintensive Aufgaben zu bewältigen, und wie Sie lokale Ereignisse und Ereignisse auf anderen Computern aufzeichnen.

Manchmal treten bei Diensten, Prozessen und Anwendungen Probleme auf. Dieses Kapitel erklärt, welche Möglichkeiten Ihnen in einem solchen Fall zur Verfügung stehen. Manchmal eignen sich die Tools, die das Betriebssystem mitbringt, nicht perfekt für diesen Zweck, daher beschreibt dieses Kapitel auch, wie Sie Standardskripts erstellen, um alle auftretenden Probleme zu behandeln. Dazu brauchen Sie keine tiefgehenden Programmierkenntnisse.

Sie müssen Dienste verwalten und konfigurieren, Auslagerungsdateien und Arbeitsspeichercache konfigurieren, Dienste konfigurieren, Prozesse verwalten, Ihren Desktop konfigurieren und (unter Umständen) Ihre Startumgebung ändern. Dieses Kapitel beschreibt all diese Aufgaben.

In diesem Kapitel abgedeckte Prüfungsziele:

- Überwachen von Systemen
- Konfigurieren von Leistungseinstellungen

Lektionen in diesem Kapitel:

- Lektion 1: Überwachen von Systemen 651
- Lektion 2: Konfigurieren von Leistungseinstellungen 693

Bevor Sie beginnen

Um die Übungen in diesem Kapitel durchzuarbeiten, müssen Sie folgende Vorbereitungen getroffen haben:

- Sie haben Windows 7 auf einem eigenständigen Client-PC installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben. Sie brauchen Internetzugriff, um die Übungen durchzuführen.
- Optional haben Sie Windows 7 auf einem zweiten PC installiert, wie in Kapitel 6, »Netzwerkeinstellungen«, beschrieben. Für die Übungen innerhalb der Lektionen brauchen Sie zwar keinen zweiten Computer, aber er ist nötig, wenn Sie die vorgeschlagenen Übungen am Ende dieses Kapitels durcharbeiten wollen.
- Falls Sie zwei physische Computer benutzen, die nicht im selben Netzwerk liegen, müssen Sie ihre Ethernetanschlüsse mit einem Crossoverkabel oder mithilfe eines Ethernetswitchs verbinden.
- Sie brauchen ein USB-Flashspeichergerät (Universal Serial Bus), auf dem mindestens 200 MByte Platz frei ist, oder eine zweite interne oder externe Festplatte.
- Der Computer, auf dem Sie die Übungen durcharbeiten (*Canberra*), muss ein optisches Laufwerk haben, das eine DVD beschreiben kann.

Praxistipp

Ian McLean

Eine Serveraufrüstung lässt sich beim Management meist recht einfach durchsetzen, selbst wenn viele Manager gar nicht wissen, was ein Server ist.

Es gibt aber gar nicht so viele Server. Dank der Virtualisierung werden es immer weniger. Es sind rätselhafte Kästen, die unverständliche Sachen machen. Wenn der Netzwerkadministrator etwas davon erzählt, dass die Server aufgerüstet werden müssen, sind die Kosten wahrscheinlich unerheblich, zumindest wenn sie im Gesamtbild betrachtet werden.

Leitende Manager kennen sich meist nicht sonderlich mit Technik aus (wenn man einen findet, jagt einem das regelrecht Angst ein), sind aber nicht dämlich, vor allem wenn es um Geld geht. Sie können die Ausgaben für die Aufrüstung eines halben Dutzends Server rechtfertigen. Aber wenn es darum geht, 500 Arbeitsstationen aufzurüsten, sieht die Sache ganz anders aus.

Daher ist es genauso wichtig, Leistungsstatistiken über Ihre Arbeitsstationen zu sammeln wie über Ihre Server. Sie können die schnellsten Server betreiben, die auf dem Markt zu haben sind, aber wenn Ihre Clientcomputer zu schwach dimensioniert sind, bietet Ihr Netzwerk schlechte Leistung. Selbst der magerste Thin-Client hat Leistungsengpässe, vor allem im Bereich der Netzwerkressourcen.

Irgendwann müssen Sie Ihre Hardware aufrüsten. Wenn nicht jetzt, dann in 1 oder 2 Jahren. Bereiten Sie sich bereits jetzt darauf vor. Stellen Sie sicher, dass Sie vernünftige Baselines definiert haben. Behalten Sie kleine, aber in ihrer Summe problematische Leistungseinbrüche im Auge, während die Hardware altert und die Anforderungen der Benutzer wachsen. Beginnen Sie noch heute damit, die Argumentation für eine Aufrüstung vorzubereiten, die in Zukunft fällig wird. Verschieben Sie das nicht auf morgen, sonst kann es Ihnen passieren, dass morgen jemand anders auf Ihrem Stuhl sitzt.

Lektion 1: Überwachen von Systemen

Als IT-Experte mit mindestens 1 Jahr Erfahrung hatten Sie sicherlich schon mit einigen, wenn nicht sogar allen Tools und Dienstprogrammen zu tun, die in dieser Lektion beschrieben werden. Windows 7 stellt unter anderem Tools zur Verfügung, die die Leistung messen, Baselines festlegen, Leistungsengpässe aufdecken, Ressourcen anzeigen oder die Systemstabilität und Zuverlässigkeit bewerten.

Manchmal ist es gar nicht so einfach, das richtige Tool für eine Aufgabe zu finden. Oft liefern mehrere Tools dieselben Informationen oder führen dieselbe Konfigurationsaufgabe aus, aber eines davon ist meist effizienter als die anderen. Es ist recht einfach, mit einem oder mehreren Tools Informationen über ein Computersystem zu sammeln. Diese Daten zu interpretieren, ist schon schwieriger. Diese Lektion versucht, die verschiedenen Tools anhand ihrer Funktion in mehrere Gruppen zu untergliedern, und beschreibt, wie sich die Tools in jeder Gruppe gegenseitig ergänzen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Benutzen von Leistungstools, um Echtzeitleistungsdaten anzuzeigen, Daten in Sammlungssätzen aufzuzeichnen und Berichte zu generieren, die tatsächliche oder potenzielle Leistungsengpässe aufdecken
- Untersuchen von Fehlern und potenziellen Problemen im Zusammenhang mit Softwareinstallationen und anderen erheblichen Änderungen am System
- Sammeln von Ereignisabonnements von Quellcomputern und Speichern der Daten auf einem Zielcomputer
- Zugreifen auf den Windows-Leistungsindex und Auswählen von Computersoftware, die sich für diesen Index eignet

Veranschlagte Zeit für diese Lektion: 50 Minuten

Systemüberwachung und Berichterstellung

Sie müssen Leistungsdaten überwachen und mit vorher ermittelten Baselines vergleichen, um den Zustand Ihrer Clientcomputer im Blick zu behalten. Außerdem müssen Sie die Ereignisse analysieren, die in den Ereignisprotokollen aufgezeichnet werden. Viele Ereignisse dienen nur Informationszwecken, aber auch solche Ereignisse sollten Sie nicht einfach ignorieren. Lassen Sie sich von Ihren Fähigkeiten und Erfahrungen als Administrator leiten, um zu entscheiden, wo Sie nachhaken müssen und was Sie problemlos ignorieren können. Was Sie niemals ignorieren sollten, sind Warnungs- und Fehlerereignisse, die oft auf echte, unmittelbare Probleme in Ihren Systemen hindeuten.

Als IT-Experte haben Sie wahrscheinlich schon Erfahrung mit den Windows-Leistungstools wie der Leistungsüberwachung und dem Berichterstellungstool gesammelt. Möglicherweise sind Sie noch nicht mit Sammlungssätzen (Data Collector Set, DCS) vertraut, die mithilfe von Leistungsindikatoren Leistungsprotokolle generieren und wiederum von der Leistungsüberwachung und dem Berichterstellungstool ausgewertet werden. Sammlungssätze sind die Nachfolger der Leistungsprotokolle und -warnungen in älteren Betriebssystemen.

Ihr Ziel besteht darin, die Leistung zu überwachen und zu optimieren, mögliche Leistungsengpässe zu identifizieren und die erforderlichen Ressourcen aufzurüsten. Vor allem müssen

Sie die Ursachen kritischer Leistungsprobleme aufdecken, die unter Umständen dazu führen, dass Dienste unerträglich langsam werden oder völlig ausfallen.

Leistungsüberwachung

In Windows 7 öffnen Sie die Leistungsüberwachung, indem Sie in der Systemsteuerung alle Systemsteuerungselemente anzeigen, auf *Leistungsinformationen und -tools* klicken, dann im Fenster *Leistungsinformationen und -tools* auf *Weitere Tools* klicken und schließlich auf *Leistungsüberwachung öffnen* klicken. Einfacher ist es, im Suchfeld des Startmenüs (oder in einer Eingabeaufforderung) **perfmon** einzugeben. Im Fenster *Leistungsüberwachung* haben Sie Zugriff auf das Tool Leistungsüberwachung, Sammlungssätze und das Berichterstellungstool. Wählen Sie in der Konsolenstruktur den Knoten *Leistungsüberwachung* aus.

Sie fügen Leistungsindikatoren hinzu, indem Sie in der Symbolleiste der Leistungsüberwachung auf die grüne Plusschaltfläche (+) klicken, das Objekt (beispielsweise *Arbeitsspeicher*) erweitern, einen Leistungsindikator auswählen und auf *Hinzufügen* klicken. Anschließend geben Sie an, ob Sie eine bestimmte Instanz eines Leistungsindikators oder eine Summe (*total*) aller Instanzen anzeigen möchten. Wenn ein Computer beispielsweise mehrere CPUs hat, haben Sie die Wahl zwischen einem Leistungsindikator, der die Auslastung einer einzelnen CPU misst, und einem, der die gesamte CPU-Auslastung misst. Abbildung 13.1 zeigt, wie die Leistungsüberwachung Echtzeitdaten anzeigt.

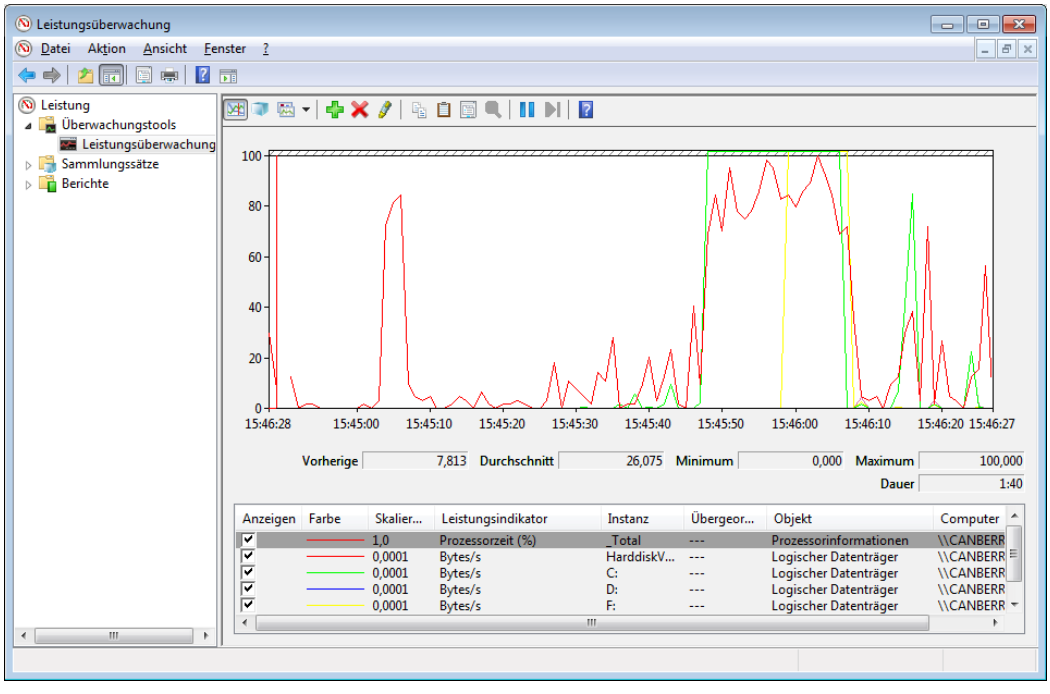


Abbildung 13.1 Anzeigen von Echtzeitdaten in der Leistungsüberwachung

Jede Kurve im Diagramm hat eine andere Farbe. Sie können eine bestimmte Kurve hervorheben, indem Sie den zugehörigen Leistungsindikator auswählen und die Tastenkombination STRG+H drücken. Der ausgewählte Leistungsindikator wird nun im Diagramm fett und in schwarzer Farbe angezeigt. Sie ändern das Aussehen und die Aktualisierungsrate des Dia-

gramms, indem Sie mit der rechten Maustaste auf *Leistungsüberwachung* klicken und den Befehl *Eigenschaften* wählen. Die fünf Registerkarten des Dialogfelds *Eigenschaften von Leistungsüberwachung* bieten Zugriff auf unterschiedliche Konfigurationsoptionen:

- **Allgemein** Im Feld *Diagrammelemente* können Sie im Feld *Stichprobe alle* ändern, wie oft das Diagramm aktualisiert wird. Sie können auch wählen, ob Legende, Wertleiste und Symbolleiste angezeigt werden und ob die Bericht- und Histogrammansichten Standard-, Maximal-, Minimal-, Durchschnitts- oder aktuelle Werte anzeigen. Abbildung 13.2 zeigt die Registerkarte *Allgemein*.

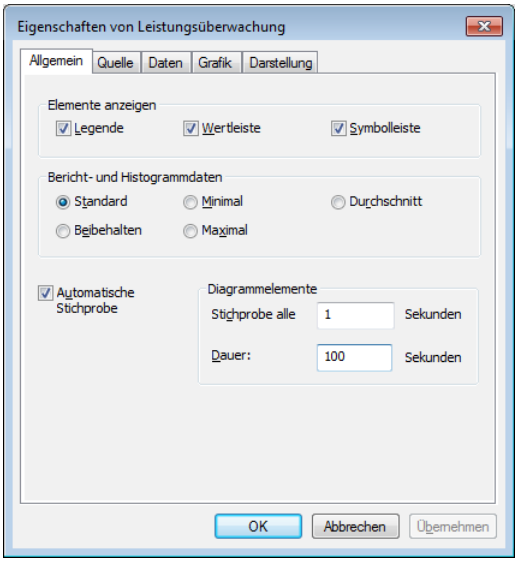


Abbildung 13.2 Die Registerkarte *Allgemein* des Dialogfelds *Eigenschaften von Leistungsüberwachung*

- **Quelle** Auf dieser Registerkarte wählen Sie, ob die aktuellen Aktivitäten in Echtzeit angezeigt werden oder Protokolldateien, die Sie vorher mit einem Sammlungssatz aufgezeichnet haben.
- **Daten** In der Liste *Leistungsindikatoren* auf dieser Registerkarte wählen Sie aus, welche Leistungsindikatoren Sie konfigurieren wollen, woraufhin Sie Farbe, Breite und Stil anpassen können.
- **Grafik** In der Standardeinstellung überschreibt die Leistungsüberwachung die dargestellten Leistungsindikatorwerte von der linken Seite des Diagramms her, sobald die angegebene Dauer überschritten ist. Wenn Sie Leistungsindikatorwerte über einen längeren Zeitraum hinweg beobachten, ist es meist sinnvoller, das Diagramm von rechts nach links zu verschieben. Wählen Sie dazu unter *Bildlaufstil* die Option *Bildlauf*. Sie können außerdem einen der folgenden Diagrammtypen auswählen, indem Sie in der Symbolleiste die Schaltfläche *Diagrammtyp ändern* anklicken oder die Tastenkombination STRG+G drücken:
  - **Linie** Dies ist die Standardeinstellung. Sie zeigt die Werte als Kurven im Diagramm an.

- **Histogrammleiste** Zeigt eine Balkengrafik an, in der die aktuellen, größten, kleinsten oder Durchschnittswerte angezeigt werden. Wenn Sie sehr viele Leistungsindikatoren haben, ist ein Histogramm einfacher zu lesen als ein Liniendiagramm.
- **Bericht** Listet die aktuellen, größten, kleinsten oder durchschnittlichen Werte der Leistungsindikatoren in einem Textbericht auf.

- **Darstellung** Wenn Sie mehrere Systemmonitorfenster gleichzeitig öffnen, können Sie auf dieser Registerkarte die Farbe des Hintergrunds oder anderer Elemente ändern.

Schnelltest

1. Auf welcher Registerkarte des Dialogfelds *Eigenschaften von Leistungsüberwachung* stellen Sie ein, wie oft das Diagramm aktualisiert wird?
2. Welche Rechte braucht ein Benutzer, um Leistungsdaten im Remotezugriff zu überwachen?

Antworten zum Schnelltest

1. Sie stellen auf der Registerkarte *Allgemein* im Feld *Diagrammelemente* den Wert im Feld *Stichprobe alle* ein, um festzulegen, wie oft das Diagramm aktualisiert wird.
2. Das Konto des Benutzers muss auf dem Remotecomputer mindestens Mitglied der Gruppen *Leistungsprotokollbenutzer* und *Ereignisprotokollleser* sein.

Sammlungssätze

Sammlungssätze (Data Collector Set, DCS) stellen Systeminformationen zusammen, darunter Konfigurationseinstellungen und Leistungsdaten, und speichern sie in einer Datendatei. Sie können eine solche Datendatei in der Leistungsüberwachung untersuchen und detaillierte Leistungsdaten analysieren, oder einen Bericht generieren, der die Daten zusammenfasst.

Windows 7 enthält die folgenden vordefinierten Sammlungssätze:

- **System Performance (Systemleistung)** Diesen Sammlungssatz können Sie einsetzen, wenn Sie eine Problembehandlung bei einem langsamen Computer oder sporadisch auftretenden Leistungseinbrüchen durchführen. Er zeichnet Prozessor-, Datenträger-, Arbeitsspeicher- und Netzwerkleistungsindikatoren (IPv4 und IPv6) sowie Kernelablaufverfolgungsdaten auf.
- **System Diagnostics (Systemdiagnose)** Diesen Sammlungssatz können Sie beim Auftreten von Zuverlässigkeitsproblemen verwenden, etwa wegen problematischer Hardware, Treiberfehlern oder Abbruchfehlern. Er zeichnet alle Informationen aus dem Sammlungssatz *System Performance (Systemleistung)* sowie detaillierte Systeminformationen auf. Abbildung 13.3 zeigt einige der Indikatoren, die im Sammlungssatz *System Diagnostics (Systemdiagnose)* enthalten sind.

Sie benutzen einen Sammlungssatz, indem Sie ihn mit der rechten Maustaste anklicken und den Befehl *Starten* wählen. Der Sammlungssatz *System Performance (Systemleistung)* zeichnet in der Standardeinstellung 10 Minuten lang Daten auf, der Sammlungssatz *System Diagnostics (Systemdiagnose)* nur 1 Minute. Sie können einen Sammlungssatz jederzeit von Hand beenden, wenn Sie ihn mit der rechten Maustaste anklicken und *Beenden* wählen.

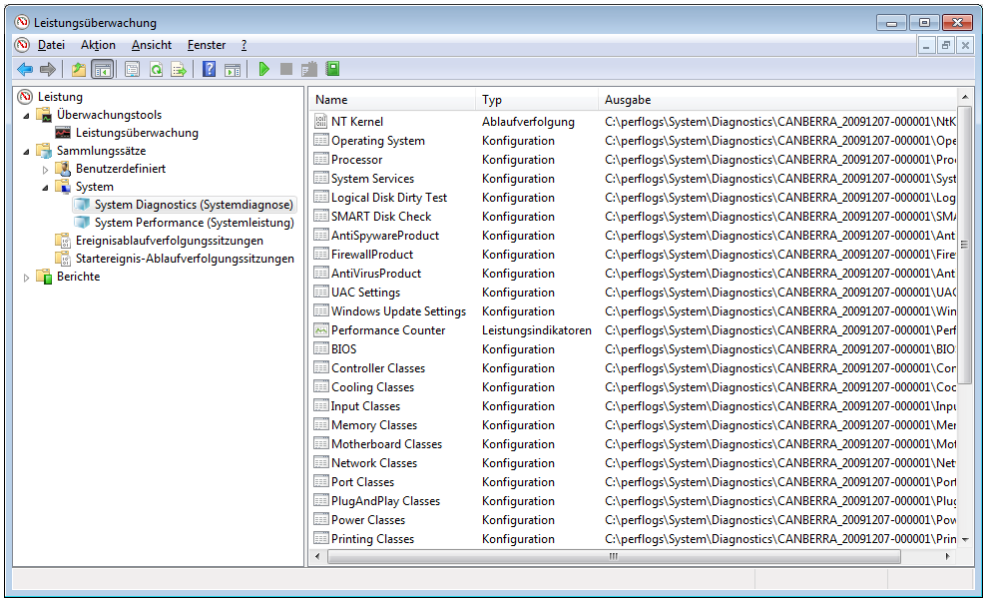


Abbildung 13.3 Indikatoren im Sammlungssatz *System Diagnostics (Systemdiagnose)*

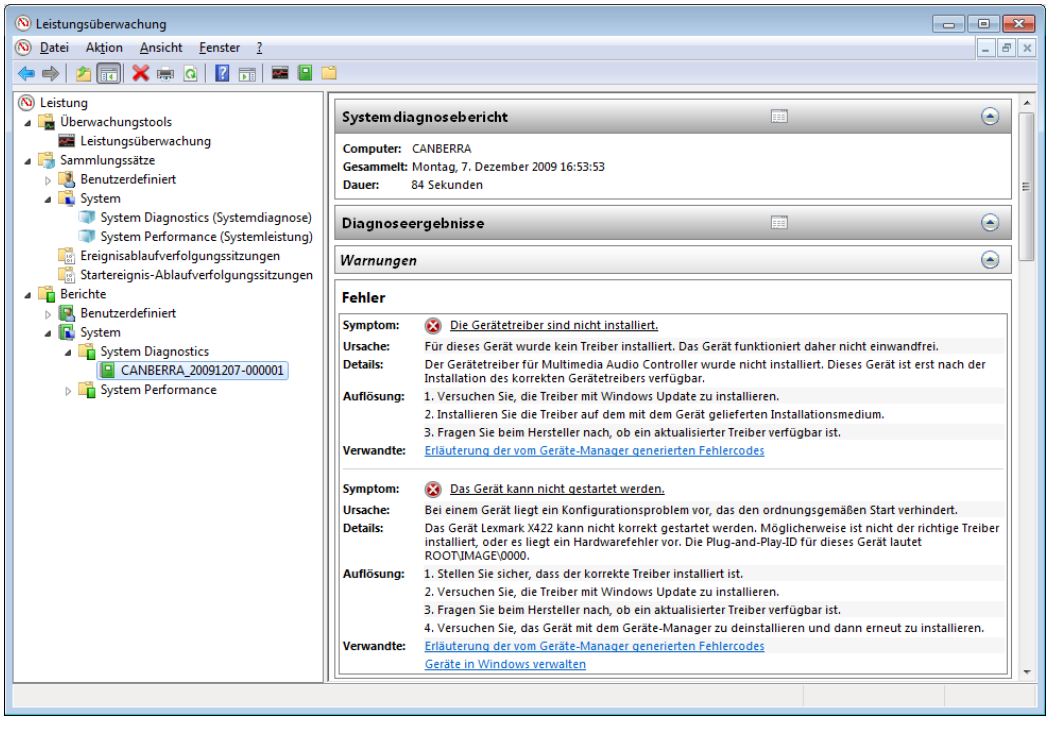

Leistungsüberwachung
Datei Aktion Ansicht Fenster ?
Leistung
Überwachungstools
Leistungsüberwachung
Sammlungssätze
Benutzerdefiniert
System
System Diagnostics (Systemdiagnose)
System Performance (Systemleistung)
Ereignisablaufverfolgungssitzungen
Startereignis-Ablaufverfolgungssitzungen
Berichte
Benutzerdefiniert
System
System Diagnostics
CANBERRA_20091207-000001
System Performance
Systemdiagnosebericht
Computer: CANBERRA
Gesammelt: Montag, 7. Dezember 2009 16:53:53
Dauer: 84 Sekunden
Diagnoseergebnisse
Warnungen
Fehler
Symptom: Die Gerätetreiber sind nicht installiert.
Ursache: Für dieses Gerät wurde kein Treiber installiert. Das Gerät funktioniert daher nicht einwandfrei.
Details: Der Gerätetreiber für Multimedia Audio Controller wurde nicht installiert. Dieses Gerät ist erst nach der Installation des korrekten Gerätetreibers verfügbar.
Auflösung: 1. Versuchen Sie, die Treiber mit Windows Update zu installieren.
2. Installieren Sie die Treiber auf dem mit dem Gerät gelieferten Installationsmedium.
3. Fragen Sie beim Hersteller nach, ob ein aktualisierter Treiber verfügbar ist.
Verwandte: Erläuterung der vom Geräte-Manager generierten Fehlercodes
Symptom: Das Gerät kann nicht gestartet werden.
Ursache: Bei einem Gerät liegt ein Konfigurationsproblem vor, das den ordnungsgemäßen Start verhindert.
Details: Das Gerät Lexmark X422 kann nicht korrekt gestartet werden. Möglicherweise ist nicht der richtige Treiber installiert, oder es liegt ein Hardwarefehler vor. Die Plug-and-Play-ID für dieses Gerät lautet ROOT\IMAGE\0000.
Auflösung: 1. Stellen Sie sicher, dass der korrekte Treiber installiert ist.
2. Versuchen Sie, die Treiber mit Windows Update zu installieren.
3. Fragen Sie beim Hersteller nach, ob ein aktualisierter Treiber verfügbar ist.
4. Versuchen Sie, das Gerät mit dem Geräte-Manager zu deinstallieren und dann erneut zu installieren.
Verwandte: Erläuterung der vom Geräte-Manager generierten Fehlercodes
Geräte in Windows verwalten

Abbildung 13.4 Öffnen eines Berichts zum Sammlungssatz *System Diagnostics (Systemdiagnose)*

Nachdem Sie einen Sammlungssatz ausgeführt haben, können Sie sich im Knoten *Leistung\Berichte* eine Zusammenfassung der gesammelten Daten ansehen. Sie zeigen den neusten

Bericht zu einem Sammlungssatz an, wenn Sie mit der rechten Maustaste auf den Sammlungssatz klicken und den Befehl *Aktuellster Bericht* wählen. Anschließend können Sie den Bericht über den Knoten *Berichte* öffnen (Abbildung 13.4).

Sie können auch Leistungsindikatorwarnungen zu Sammlungssätzen hinzufügen. Auf diese Weise können Sie eine Warnung definieren und auslösen lassen, mit der Sie beispielsweise eine Batchdatei starten, eine E-Mail versenden oder einen Pager anrufen. Wenn Sie beispielsweise eine Warnung konfiguriert haben, die ausgelöst wird, sobald der freie Platz auf einem logischen Volume unter den Wert von 30 Prozent fällt, können Sie diese Warnung zu einem Sammlungssatz hinzufügen und damit eine Batchdatei auslösen, die die Daten auf dem Volume archiviert.

Die Datenprotokollierung verbraucht viele Systemressourcen, und Leistungsprotokolldateien können sehr groß werden. Um die Leistungsauswirkungen durch die Leistungsdatenprotokollierung so gering wie möglich zu halten, sollten Sie nur die Daten aufzeichnen, die Sie tatsächlich benötigen. Zum Beispiel sollten Sie nach Möglichkeit *System Performance (Systemleistung)* statt *System Diagnostics (Systemdiagnose)* benutzen, weil *System Performance* weniger Leistungsindikatoren enthält.

Erstellen eines Sammlungssatzes

Wenn Sie ein Leistungsproblem haben oder die Leistung eines Clientcomputers analysieren und möglicherweise verbessern wollen, können Sie mit Sammlungssätzen Leistungsdaten aufzeichnen und mit Ihren Baselines vergleichen. Sie gehen folgendermaßen vor, um einen benutzerdefinierten Sammlungssatz zusammenzustellen:

1. Erweitern Sie in der Konsole *Leistungsüberwachung* (nicht im gleichnamigen Tool innerhalb dieser Konsole) den Knoten *Sammlungssätze*, klicken Sie mit der rechten Maustaste auf *Sammlungssätze\Benutzerdefiniert* und wählen Sie den Befehl *Neu/Sammlungssatz*. Daraufhin öffnet sich der Assistent *Neuen Sammlungssatz erstellen*.
2. Geben Sie auf der Seite *Wie soll dieser neue Sammlungssatz erstellt werden* einen Namen für den Sammlungssatz ein. Stellen Sie sicher, dass die Option *Aus Vorlage erstellen (empfohlen)* ausgewählt ist. Klicken Sie auf *Weiter*.
3. Wählen Sie auf der Seite *Welche Vorlage möchten Sie verwenden* die gewünschte Standardvorlage aus (*Basis*, *System Diagnostics* oder *System Performance*). Klicken Sie auf *Weiter*.
4. Klicken Sie auf der Seite *Wo sollen die Daten gespeichert werden* auf *Weiter*, um den Standardspeicherort für die Daten zu verwenden.
5. Lassen Sie auf der Seite *Möchten Sie den Sammlungssatz erstellen* im Feld *Ausführen als* den Eintrag *<Standard>* eingetragen, wenn der Sammlungssatz unter dem Konto des angemeldeten Benutzers ausgeführt werden soll. Stattdessen können Sie auch auf die Schaltfläche *Ändern* klicken und alternative administrative Anmeldeinformationen eingeben.
6. Wählen Sie eine der drei folgenden Optionen aus, bevor Sie die Schaltfläche *Fertig stellen* anklicken:
   - *Eigenschaften für diesen Sammlungssatz öffnen*
   - *Diesen Sammlungssatz jetzt starten*
   - *Speichern und schließen*

Benutzerdefinierte Sammlungssätze liegen im Knoten *Benutzerdefiniert* unterhalb von *Sammlungssätze*. Sie können einen Zeitplan festlegen, der steuert, wann ein Sammlungssatz startet, und seine Stoppbedingungen konfigurieren. Sie starten einen Sammlungssatz von Hand, indem Sie ihn mit der rechten Maustaste anklicken und den Befehl *Starten* wählen.



Weitere Informationen Erstellen von Sammlungssätzen

Weitere Informationen über die verschiedenen Methoden zum Erstellen von Sammlungssätzen finden Sie unter *http://technet.microsoft.com/de-de/library/cc749337.aspx*.

Anpassen von Sammlungssätzen

Ein benutzerdefinierter Sammlungssatz zeichnet die Leistungsdaten auf, die in der verwendeten Vorlage definiert sind. Wenn Sie Ihre eigenen Datenquellen zu einem Sammlungssatz hinzufügen, müssen Sie ihn anschließend aktualisieren.

Sie fügen eine Leistungsdatenquelle (etwa einen Leistungsindikator) zu einem Sammlungssatz hinzu, indem Sie mit der rechten Maustaste auf den Sammlungssatz klicken und den Befehl *Neu/Sammlung* wählen. Daraufhin öffnet sich der Assistent *Neue Sammlung erstellen*. Geben Sie auf der Seite *Welche Art von Datensammler möchten Sie erstellen* einen Namen für die Sammlung ein, wählen Sie den Typ aus und klicken Sie auf *Weiter*. Es stehen folgende Sammlungstypen zur Wahl:

- **Leistungsindikatorensammlung** Mit diesem Sammlungstyp sammeln Sie Leistungsstatistiken über längere Zeiträume, um sie später zu analysieren. Sie können damit Baselines messen und Trends analysieren.
- **Ereignisablaufverfolgungssammlung** Mit diesem Sammlungstyp zeichnen Sie Informationen über Systemereignisse und -aktivitäten auf.
- **Konfigurationssammlung** Dieser Sammlungstyp speichert Informationen über Registrierungsschlüssel, WMI-Verwaltungspfade (Windows Management Instrumentation) und den Systemzustand.
- **Leistungsindikatorenwarnung** Mit diesem Sammlungstyp konfigurieren Sie eine Warnung, die ausgelöst wird, sobald ein bestimmter Leistungsindikator einen festgelegten Schwellenwert unter- oder überschreitet.

Sie können beliebig viele Sammlungen zu einem Sammlungssatz hinzufügen. Sie bearbeiten eine Sammlung, indem Sie den entsprechenden Eintrag im Knoten *Sammlungssätze\Benutzerdefiniert* auswählen, die Sammlung in der Detailansicht mit der rechten Maustaste anklicken und den Befehl *Eigenschaften* wählen.



Weitere Informationen Eigenschaften von Sammlungssätzen

Weitere Informationen darüber, wie Sie die Eigenschaften von Sammlungssätzen konfigurieren, finden Sie unter *http://technet.microsoft.com/de-de/library/cc749267.aspx*.

Wenn ein Sammlungssatz Leistungsindikatoren enthält, können Sie sich die Leistungsindikatorwerte in der Leistungsüberwachung ansehen, wenn Sie mit der rechten Maustaste auf den Bericht klicken und den Befehl *Ansicht/Leistungsüberwachung* wählen. Die Leistungsüberwachung zeigt daraufhin nicht mehr die Echtzeitdaten an, sondern die Daten, die der Sammlungssatz aufgezeichnet hat.

Erstellen von Sammlungen über die Befehlszeile

Sie können Sammlungen auch in einer Eingabeaufforderung mit erhöhten Rechten erstellen. Dafür steht das Tool Logman zur Verfügung. Unter anderem stehen folgende Befehle zur Verfügung, um die verschiedenen Sammlungstypen zu erstellen, die im letzten Abschnitt aufgeführt wurden:

- **logman create counter** Dieser Befehl erstellt eine Leistungsindikatorensammlung. Zum Beispiel erstellt der Befehl `logman create counter my_perf_log -c "\Processor(_Total)\% Processor Time"` einen Leistungsindikatorsammlungssatz namens *my_perf_log*, der Werte der Leistungsindikatorinstanz *Prozessor(_Total)* des Leistungsindikators *Prozessorzeit (%)* aufzeichnet.
- **logman create trace** Dieser Befehl erstellt eine Ereignisablaufverfolgungssammlung. Zum Beispiel erstellt der Befehl `logman create trace my_trace_log -o c:\trace_log_file` eine Ereignisablaufverfolgungssammlung namens *my_trace_log*, die ihre Ergebnisse in *c:\trace_log_file* schreibt.
- **logman create config** Dieser Befehl erstellt eine Konfigurationssammlung. Zum Beispiel erstellt der Befehl `logman create config my_cfg_log -reg HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\\` eine Konfigurationssammlung namens *my_cfg_log using* für den Registrierungsschlüssel *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion*.
- **logman create alert** Dieser Befehl erstellt eine Warnungssammlung. Zum Beispiel erstellt der Befehl `logman create alert my_alert -th "\Processor(_Total)\% Processor Time>90"` eine Warnung namens *my_alert*, die ausgelöst wird, sobald die Leistungsindikatorinstanz *Prozessor(_Total)* des Leistungsindikators *Prozessorzeit (%)* den Wert 90 überschreitet.

Mit dem Tool Logman können Sie auch die Ausgaben einer Sammlung abfragen. So listet beispielsweise der Befehl `logman query "my_perf_log"` die Sammlungen im Sammlungssatz *my_perf_log* auf. Sie können mit dem Tool Sammlungssätze starten und anhalten, die Befehle lauten beispielsweise `logman start my_perf_log` und `logman stop my_perf_log`. Mit dem Befehl `logman delete my_perf_log` löschen Sie den angegebenen Sammlungssatz, und mit `logman update` aktualisieren Sie einen Leistungsindikator, einen Ablaufverfolgungsleistungsindikator, eine Warnung oder eine Konfiguration. Mit Logman können Sie die Daten aus Sammlungssätzen in eine XML-Datei exportieren und aus einer solchen Datei importieren.



Weitere Informationen Logman

Weitere Informationen über das Tool Logman finden Sie unter *http://technet.microsoft.com/en-us/library/cc753820.aspx*.

Generieren eines Systemdiagnoseberichts

Wenn Sie einen Sammlungssatz erstellen und aufzeichnen, wird ein Bericht generiert, den Sie sich in der Konsole *Leistungsüberwachung* im Zweig *Berichte/Benutzerdefiniert* ansehen können. Das Berichterstellungstool enthält aber auch einen Systemdiagnosebericht, manchmal auch als *Computerintegritätsprüfung* oder »computer health check« bezeichnet (auch wenn der Begriff *Integritätsprüfung* eher auf Servern als auf Clientcomputern benutzt wird).

Ein Systemdiagnosebericht liefert Ihnen Details über den Status von Hardwareressourcen, Systemreaktionszeiten und Prozessen auf dem lokalen Computer sowie Systeminformationen

und Konfigurationsdaten. Sie generieren einen Systemdiagnosebericht üblicherweise, wenn Sie nach Möglichkeiten suchen, die Leistung zu verbessern und das System zu optimieren. Sie müssen Mitglied der lokalen Gruppe *Administratoren* sein oder entsprechende Berechtigungen haben, um einen Systemdiagnosebericht zu generieren.

Wenn Sie sich in der Konsole *Leistungsüberwachung* den Systemdiagnosebericht ansehen, erhalten Sie die Version des Berichts, die den Zeitpunkt beschreibt, als der Bericht zum letzten Mal generiert wurde. Geben Sie den folgenden Befehl ins Suchfeld des Startmenüs ein, um einen Systemdiagnosebericht zu generieren und anzuzeigen, der auf dem neusten Stand ist:

```
perfmon /report
```

Wenn es Ihnen lieber ist, können Sie `perfmon.exe /report` stattdessen auch in einer Eingabeaufforderung mit erhöhten Rechten ausführen. In beiden Fällen generiert der Befehl einen Diagnosebericht (das dauert gewöhnlich etwa 60 Sekunden) und zeigt ihn im Fenster *Ressourcen- und Leistungsüberwachung* an (Abbildung 13.5). Nun können Sie den Bericht durchblättern und die verschiedenen Abschnitte aufklappen.

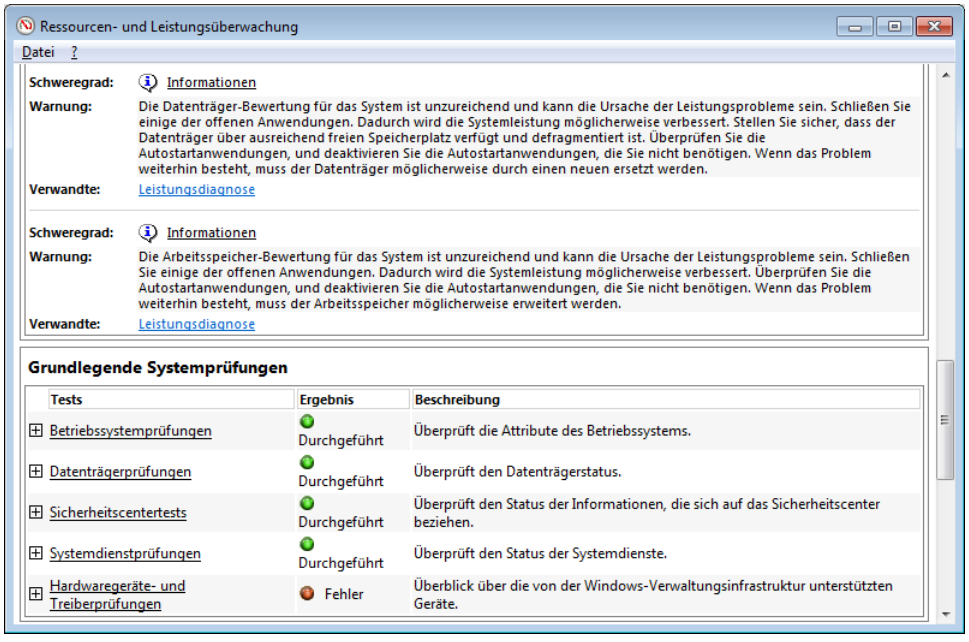
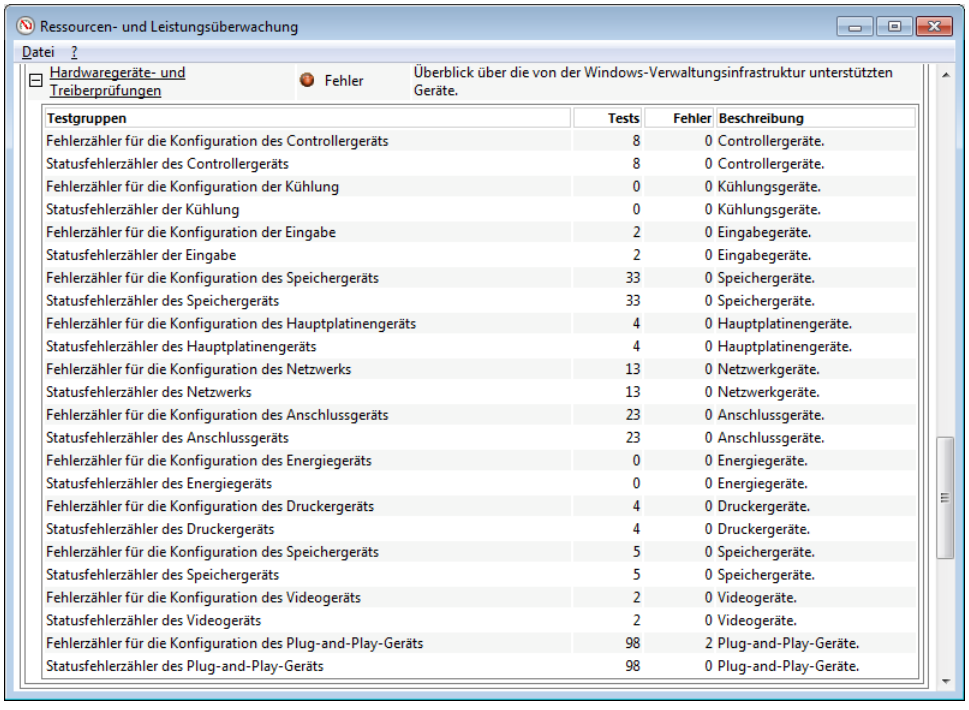

Ressourcen- und Leistungsüberwachung
Datei ?
Schweregrad: Informationen
Warnung: Die Datenträger-Bewertung für das System ist unzureichend und kann die Ursache der Leistungsprobleme sein. Schließen Sie einige der offenen Anwendungen. Dadurch wird die Systemleistung möglicherweise verbessert. Stellen Sie sicher, dass der Datenträger über ausreichend freien Speicherplatz verfügt und defragmentiert ist. Überprüfen Sie die Autostartanwendungen, und deaktivieren Sie die Autostartanwendungen, die Sie nicht benötigen. Wenn das Problem weiterhin besteht, muss der Datenträger möglicherweise durch einen neuen ersetzt werden.
Verwandte: Leistungsdiagnose
Schweregrad: Informationen
Warnung: Die Arbeitsspeicher-Bewertung für das System ist unzureichend und kann die Ursache der Leistungsprobleme sein. Schließen Sie einige der offenen Anwendungen. Dadurch wird die Systemleistung möglicherweise verbessert. Überprüfen Sie die Autostartanwendungen, und deaktivieren Sie die Autostartanwendungen, die Sie nicht benötigen. Wenn das Problem weiterhin besteht, muss der Arbeitsspeicher möglicherweise erweitert werden.
Verwandte: Leistungsdiagnose
Grundlegende Systemprüfungen
Tests
Ergebnis
Beschreibung
Betriebssystemprüfungen
Durchgeführt
Überprüft die Attribute des Betriebssystems.
Datenträgerprüfungen
Durchgeführt
Überprüft den Datenträgerstatus.
Sicherheitscentertests
Durchgeführt
Überprüft den Status der Informationen, die sich auf das Sicherheitscenter beziehen.
Systemdienstprüfungen
Durchgeführt
Überprüft den Status der Systemdienste.
Hardwaregeräte- und Treiberprüfungen
Fehler
Überblick über die von der Windows-Verwaltungsinfrastruktur unterstützten Geräte.

Abbildung 13.5 Der Systemdiagnosebericht in der Ressourcen- und Leistungsüberwachung

Wenn Sie beispielsweise im Abschnitt *Grundlegende Systemprüfungen* den Zweig *Hardwaregeräte- und Treiberprüfungen* aufklappen, erhalten Sie Informationen wie in Abbildung 13.6. Hier sind unter anderem Probleme mit Plug & Play-Geräten aufgeführt.

Es gibt die Abschnitte *Leistung*, *Softwarekonfiguration*, *Hardwarekonfiguration*, *CPU*, *Netzwerk*, *Datenträger*, *Arbeitsspeicher* und *Berichtstatistik*. Unter *Softwarekonfiguration* finden Sie ausführliche Informationen (Abbildung 13.7) zu verschiedenen Bereichen wie Betriebssystem oder Sicherheit. Wurde ein Fehler gefunden, können Sie ihn genauer untersuchen, indem Sie auf den mit einem Plussymbol markierten Knoten klicken.



Testgruppen	Tests	Fehler	Beschreibung
Fehlerzähler für die Konfiguration des Controllergeräts	8	0	Controllergeräte.
Statusfehlerzähler des Controllergeräts	8	0	Controllergeräte.
Fehlerzähler für die Konfiguration der Kühlung	0	0	Kühlungsgeräte.
Statusfehlerzähler der Kühlung	0	0	Kühlungsgeräte.
Fehlerzähler für die Konfiguration der Eingabe	2	0	Eingabegeräte.
Statusfehlerzähler der Eingabe	2	0	Eingabegeräte.
Fehlerzähler für die Konfiguration des Speichergeräts	33	0	Speichergeräte.
Statusfehlerzähler des Speichergeräts	33	0	Speichergeräte.
Fehlerzähler für die Konfiguration des Hauptplatinengeräts	4	0	Hauptplatinengeräte.
Statusfehlerzähler des Hauptplatinengeräts	4	0	Hauptplatinengeräte.
Fehlerzähler für die Konfiguration des Netzwerks	13	0	Netzwerkgeräte.
Statusfehlerzähler des Netzwerks	13	0	Netzwerkgeräte.
Fehlerzähler für die Konfiguration des Anschlussgeräts	23	0	Anschlussgeräte.
Statusfehlerzähler des Anschlussgeräts	23	0	Anschlussgeräte.
Fehlerzähler für die Konfiguration des Energiegeräts	0	0	Energiegeräte.
Statusfehlerzähler des Energiegeräts	0	0	Energiegeräte.
Fehlerzähler für die Konfiguration des Druckergeräts	4	0	Druckergeräte.
Statusfehlerzähler des Druckergeräts	4	0	Druckergeräte.
Fehlerzähler für die Konfiguration des Speichergeräts	5	0	Speichergeräte.
Statusfehlerzähler des Speichergeräts	5	0	Speichergeräte.
Fehlerzähler für die Konfiguration des Videogeräts	2	0	Videogeräte.
Statusfehlerzähler des Videogeräts	2	0	Videogeräte.
Fehlerzähler für die Konfiguration des Plug-and-Play-Geräts	98	2	Plug-and-Play-Geräte.
Statusfehlerzähler des Plug-and-Play-Geräts	98	0	Plug-and-Play-Geräte.

Abbildung 13.6 Anzeigen von Hardwaregeräte- und Treiberprüfungen

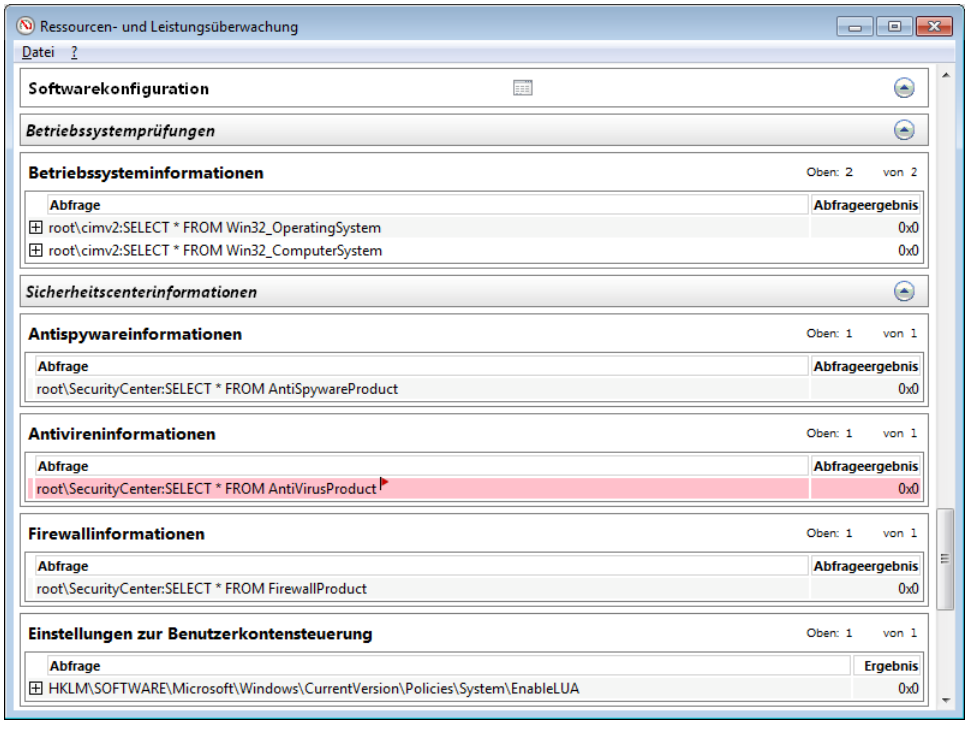


Abbildung 13.7 Informationen zur Softwarekonfiguration im Systemdiagnosebericht

Wenn Sie *Berichtstatistik* erweitern, erhalten Sie Informationen zum Computer und den Dateien. Außerdem sind hier die verarbeiteten Ereignisse mit ihren Nutzlast-GUIDs aufgelistet (Abbildung 13.8).

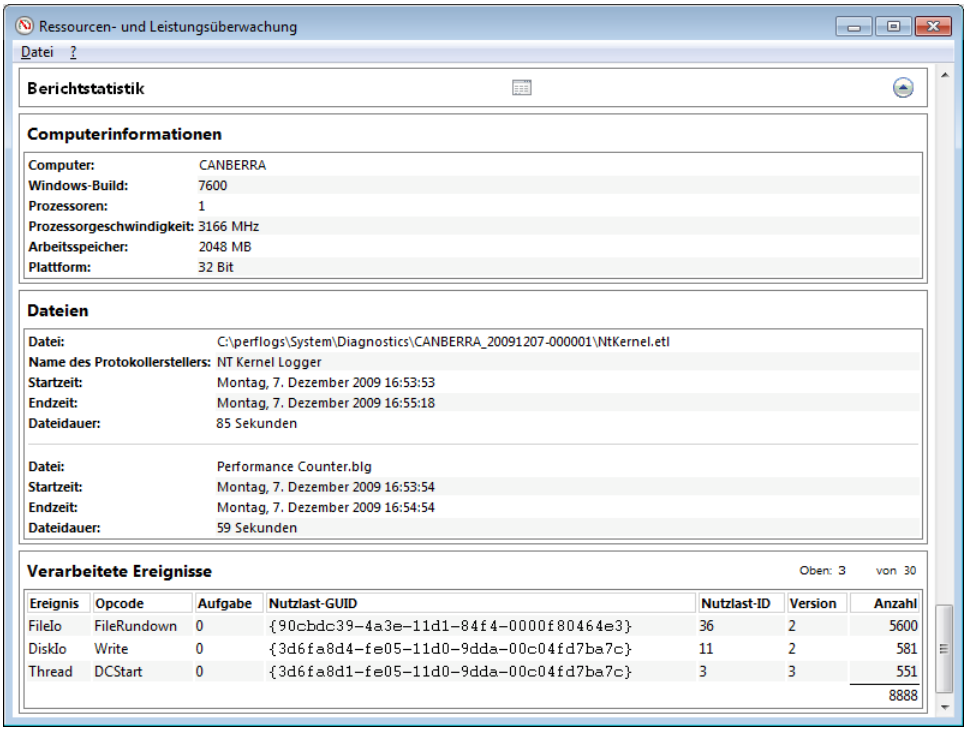


Abbildung 13.8 Der Zweig *Berichtstatistik* im Systemdiagnosebericht

Verfolgen von Zuverlässigkeit, Stabilität und Gesamtleistung des Systems

Windows 7 stellt mehrere Tools zur Verfügung, um die Zuverlässigkeit und Stabilität des Systems zu überwachen. Die Zuverlässigkeitsüberwachung verfolgt Softwareänderungen und Updates, damit Sie einen möglichen Zusammenhang zwischen Systemänderungen und Abstürzen oder Neustarts erkennen. Das Wartungscenter überwacht Ihren Computer und meldet Probleme in den Bereichen Sicherheit, Wartung und zugehörigen Diensten. Und der Windows-Leistungsindex misst die Fähigkeiten der Hardware- und Softwarekonfiguration Ihres Computers und bewertet sie mit einer Note.

Zuverlässigkeitsüberwachung

Die Zuverlässigkeitsüberwachung verfolgt die Stabilität eines Computers. Computer, die nicht neu gestartet werden und keine Fehler verursachen, werden als stabil eingestuft und erreichen (nach einiger Zeit) den maximalen Stabilitätsindex 10. Je mehr Neustarts oder Fehler auf einem Computer stattfinden, desto niedriger wird die Systemstabilität. Der kleinstmögliche Indexwert ist 0. Der Stabilitätsindex ist kein exaktes Maß für die Zuverlässigkeit, weil manchmal die Installation eines neuen Service Packs oder eines Updates einen Neustart erfordert, was den Indexwert erst einmal senkt, das System aber letztlich zuverlässiger macht,

als es zuvor war. Die Zuverlässigkeitsüberwachung liefert aber wertvolle Informationen darüber, welche Änderungen am System vorgenommen wurden, bevor ein Problem auftrat. Am einfachsten starten Sie die Zuverlässigkeitsüberwachung, indem Sie im Suchfeld des Startmenüs **perfmon /rel** eingeben.

Die Zuverlässigkeitsüberwachung eignet sich, um sporadisch auftretende Probleme zu diagnostizieren. Wenn Sie beispielsweise eine Anwendung installieren, die dazu führt, dass das Betriebssystem gelegentlich abstürzt, ist es schwierig, den Zusammenhang zwischen den Abstürzen und der Anwendungsinstallation herzustellen. Abbildung 13.9 zeigt, wie die Zuverlässigkeitsüberwachung darauf hinweist, dass nach einer Treiberinstallation ein Stabilitätseinbruch auftrat. Wenn Sie dieses Ergebnis in einem Testnetzwerk bekommen, sollten Sie sich überlegen, ob Sie sich nicht lieber mehr Informationen besorgen, bevor Sie den Treiber in Ihrem Produktivnetzwerk aktualisieren.

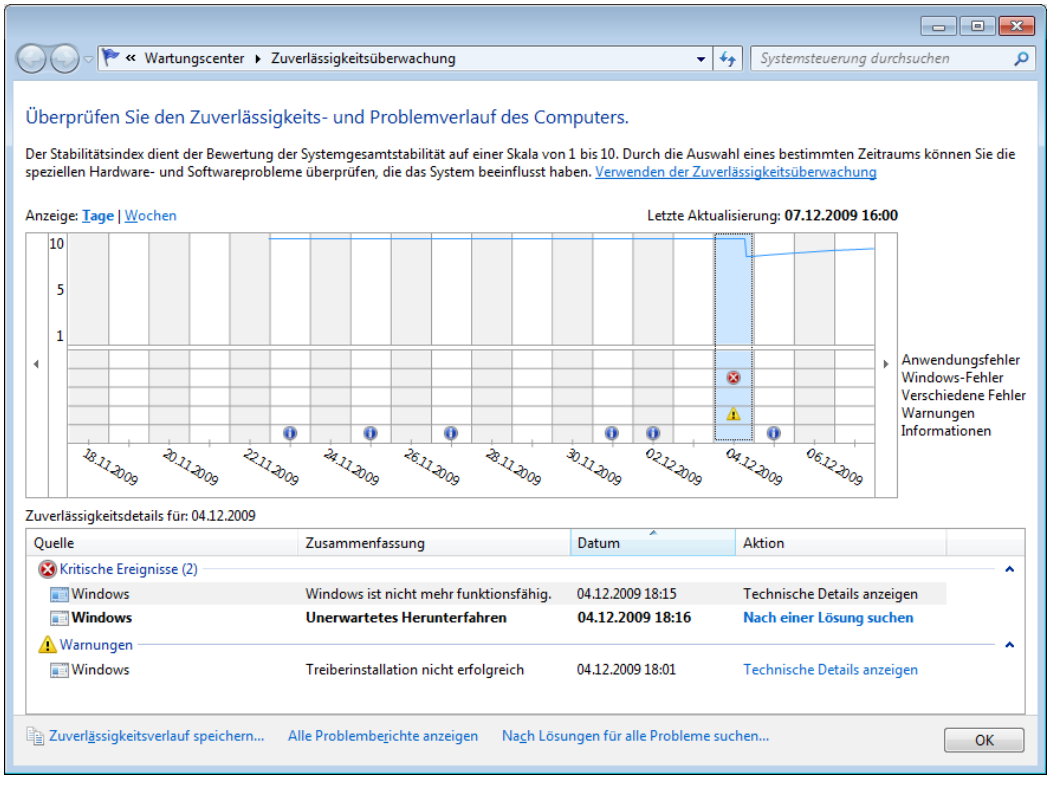


Abbildung 13.9 Zuverlässigkeitsüberwachung

Der Stabilitätsindex

Der Stabilitätsindex basiert auf Daten, die über die gesamte Lebensdauer eines Systems hinweg gesammelt werden. Zu jedem Tag wird im Systemstabilitätsdiagramm der jeweilige Stabilitätsindex angezeigt. Der Stabilitätsindex ist ein gewichtetes Maß, das aus der Zahl der Fehler über einen bestimmten, immer gleich langen Zeitraum berechnet wird. Der Indexwert wird dabei über die letzten 28 Tage berechnet, auch wenn die Ergebnisse für einen deutlich längeren Zeitraum angezeigt werden können.

Vor Kurzem aufgetretene Fehler bekommen mehr Gewicht zugemessen als länger zurückliegende Fehler. Daher macht sich eine Verbesserung durch einen langsam ansteigenden Stabilitätsindex bemerkbar, nachdem ein Zuverlässigkeitsproblem beseitigt wurde. Tage, an denen der Computer ausgeschaltet oder im Ruhezustand war, werden zur Berechnung des Stabilitätsindex nicht herangezogen.

Stehen nicht genug Daten zur Verfügung, um einen verlässlichen Stabilitätsindex zu berechnen, wird eine gepunktete Kurve im Diagramm angezeigt. Bis die Zuverlässigkeitsüberwachung Daten für 28 Tage zur Verfügung hat, wird der Stabilitätsindex daher als gepunktete Kurve angezeigt, was zeigt, dass noch keine gültige Baseline vorhanden ist. Sobald genug Daten aufgezeichnet wurden, um einen zuverlässigen Stabilitätsindex zu generieren, wird die Kurve durchgezogen. Falls sich die Systemzeit stark verändert, wird im Diagramm an den entsprechenden Tagen ein Informationssymbol angezeigt.

Die Zuverlässigkeitsüberwachung zeichnet die Stabilitäts- und Zuverlässigkeitsereignisse eines Jahres auf. Das Stabilitätsdiagramm zeigt die Daten über einer Datumsachse an.

Schnelltest

- Was bedeutet der Stabilitätsindex 10?

Antwort zum Schnelltest

- 10 ist der höchste Wert für den Stabilitätsindex. Er bedeutet, dass der Computer während der letzten 28 Tage stabil war und dass keine Fehler oder Neustarts vorgekommen sind. Er bedeutet außerdem, dass während dieser Zeit keine Softwareupdates und Service Packs eingespielt wurden, die einen Neustart erfordern.

Das Stabilitätsdiagramm

Das Stabilitätsdiagramm in der Zuverlässigkeitsüberwachung zeigt eine Kurve des Stabilitätsindex an, wobei für jeden Tag ein Datenpunkt eingezeichnet ist. Symbole in der unteren Hälfte des Diagramms stehen für Zuverlässigkeitsereignisse, die sich entweder auf die Stabilitätsmessung des Systems auswirken oder Informationen über Softwareinstallation und -deinstallation liefern. Wird an einem Tag ein Zuverlässigkeitsereignis des entsprechenden Typs erkannt, erscheint ein Symbol in der Spalte zu diesem Datum.

Bei Softwareinstallationen und -deinstallationen zeigt ein Informationssymbol ein erfolgreiches Ereignis an, bei einem Fehler ein Warnsymbol. Bei allen anderen Zuverlässigkeitsereignistypen zeigt ein Fehlersymbol einen Fehler an. Stehen Daten für mehr als 30 Tage zur Verfügung, können Sie das Stabilitätsdiagramm mit den Cursortasten der Tastatur verschieben, um sich andere Zeiträume anzusehen.

Arbeiten mit dem Wartungscenter

Das Wartungscenter, das Sie in der Systemsteuerung unter *System und Sicherheit* öffnen, überwacht Ihren Computer und meldet Probleme aus den Bereichen Sicherheit, Wartung und zugehörigen Einstellungen, die dabei helfen, die Gesamtleistung Ihres Computers zu ermitteln. Es benachrichtigt Benutzer, wenn ein Problem mit der Firewall, der Antivirensoftware, der Antispywaresoftware oder Windows Update auf ihrem Windows 7-Computer auftritt. Ändert sich der Status eines überwachten Elements (weil beispielsweise Ihre Antivirensoftware veraltet ist), benachrichtigt das Wartungscenter Sie mithilfe einer Meldung im Info-

bereich der Taskleiste. Der Status des entsprechenden Elements im Wartungscenter ändert die Farbe, um den Schweregrad der Meldung sichtbar zu machen, und das Wartungscenter empfiehlt eine Maßnahme. Abbildung 13.10 zeigt das Wartungscenter.

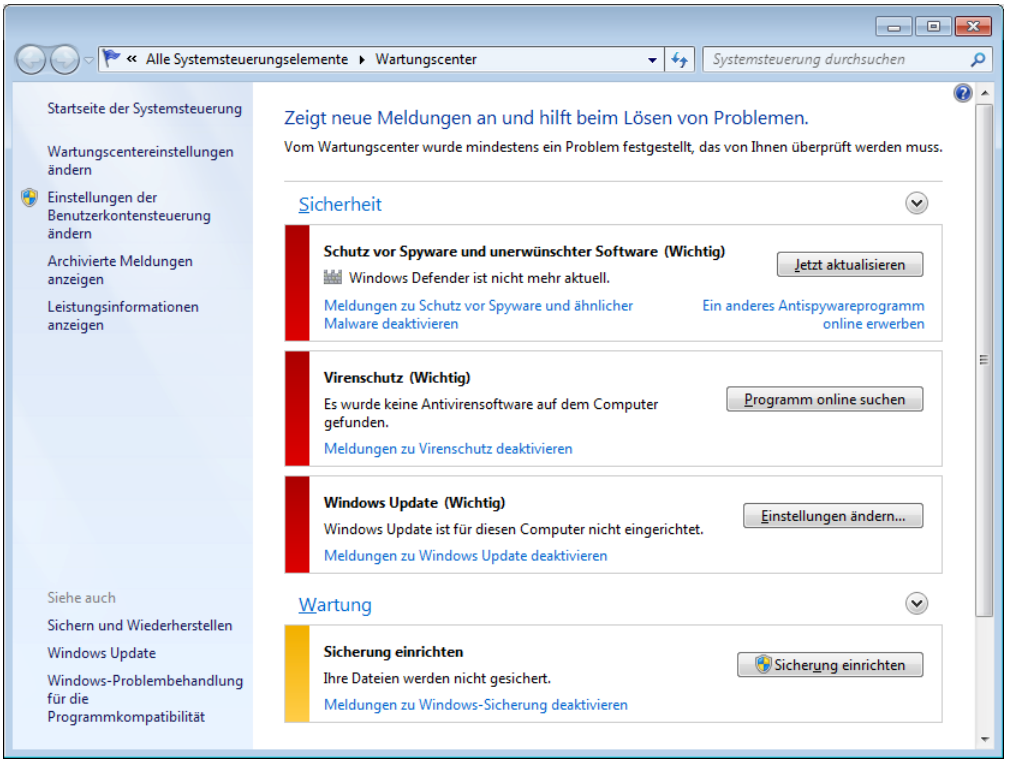

« Alle Systemsteuerungselemente ▸ Wartungscenter
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Wartungscentereinstellungen ändern
Einstellungen der Benutzerkontensteuerung ändern
Archivierte Meldungen anzeigen
Leistungsinformationen anzeigen
Zeigt neue Meldungen an und hilft beim Lösen von Problemen.
Vom Wartungscenter wurde mindestens ein Problem festgestellt, das von Ihnen überprüft werden muss.
Sicherheit
Schutz vor Spyware und unerwünschter Software (Wichtig)
Windows Defender ist nicht mehr aktuell.
Jetzt aktualisieren
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Ein anderes Antispywareprogramm online erwerben
Virenschutz (Wichtig)
Es wurde keine Antivirensoftware auf dem Computer gefunden.
Programm online suchen
Meldungen zu Virenschutz deaktivieren
Windows Update (Wichtig)
Windows Update ist für diesen Computer nicht eingerichtet.
Einstellungen ändern...
Meldungen zu Windows Update deaktivieren
Siehe auch
Sichern und Wiederherstellen
Windows Update
Windows-Problembehandlung für die Programmkompatibilität
Wartung
Sicherung einrichten
Ihre Dateien werden nicht gesichert.
Sicherung einrichten
Meldungen zu Windows-Sicherung deaktivieren

Abbildung 13.10 Das Wartungscenter

Ändern von Wartungscentereinstellungen

Wenn Sie ein Element lieber selbst im Auge behalten und keine Benachrichtigungen über seinen Status angezeigt bekommen wollen, können Sie die Benachrichtigungen für das Element im Dialogfeld *Wartungscentereinstellungen ändern* ausschalten (Abbildung 13.11).

Wenn Sie das Kontrollkästchen eines Elements im Dialogfeld *Wartungscentereinstellungen ändern* deaktivieren, bekommen Sie keine Meldungen mehr darüber, und sein Status wird nicht mehr im Wartungscenter angezeigt. Microsoft empfiehlt, den Status aller aufgelisteten Elemente zu überprüfen, weil Sie auf diese Weise vor Sicherheitsproblemen gewarnt werden.

Der Windows-Leistungsindex

Im Wartungscenter können Sie Meldungen archivieren und sich archivierte Meldungen ansehen. Sie können einen Link anklicken, um die Einstellung der Benutzerkontensteuerung zu ändern, wie in Kapitel 9, »Authentifizierung und Benutzerkontensteuerung«, beschrieben. Wenn Sie die aktuelle Leistung des Computers ermitteln wollen, ist der nützlichste Link im Wartungscenter *Leistungsinformationen anzeigen*; er zeigt den Windows-Leistungsindex im Fenster *Leistungsinformationen und -tools* an (Abbildung 13.12).

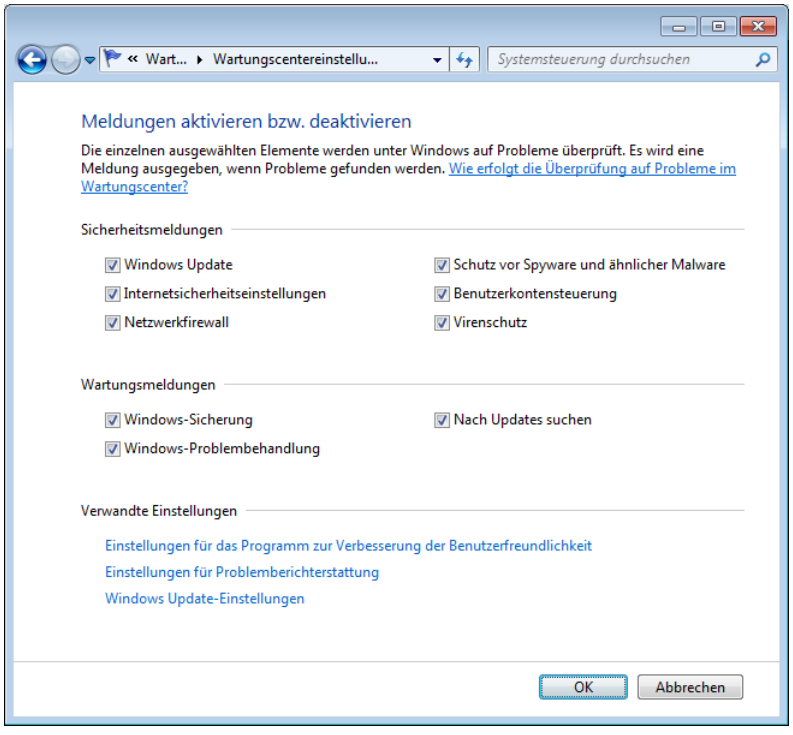


Abbildung 13.11 Das Dialogfeld *Wartungscentereinstellungen ändern*


« Alle Systemsteuerungselem... ▸ Leistungsinformationen und -tools
Systemsteuerung durchsuchen
Startseite der Systemsteuerung
Visuelle Effekte anpassen
Indizierungsoptionen anpassen
Energieeinstellungen anpassen
Datenträgerbereinigung öffnen
Weitere Tools
Bewertung und Verbesserung der Leistung des Computers
Mithilfe des Windows-Leistungsindex werden wichtige Systemkomponenten anhand einer Skala von 1,0 bis 7,9 bewertet.
Komponente | Was wurde bewertet | Teilbewertung | Gesamtbewertung
Prozessor: | Berechnungen pro Sekunde | 6,5
Arbeitsspeicher (RAM): | Speichervorgänge pro Sekunde | 6,8
Grafik: | Desktopleistung für Windows Aero | 3,5
Grafik (Spiele): | 3D-Business- und Gaminggrafikleistung | 5,7
Primäre Festplatte: | Datentransferrate | 5,2
3,5
Ergibt sich aus der niedrigsten Teilbewertung
Was bedeuten diese Werte?
Tipps zum Verbessern der Leistung des Computers
Detaillierte Leistungs- und Systeminformationen anzeigen und drucken
Weitere Informationen zu Bewertungen und Software online anzeigen
Siehe auch
Wartungscenter
Die Bewertungen sind aktuell.
Letzte Aktualisierung: 14.11.2009 11:24:56
Bewertung erneut ausführen

Abbildung 13.12 Der Windows-Leistungsindex

Der Windows-Leistungsindex misst die Fähigkeiten der Hardware- und Softwarekonfiguration Ihres Computers und berechnet daraus einen Notenwert. Je höher die Gesamtbewertung, desto schneller ist Ihr Computer im Allgemeinen bei der Durchführung ressourcenintensiver Aufgaben.

Jede Hardwarekomponente erhält eine separate Teilnote, und die Gesamtbewertung ergibt sich aus der schlechtesten Teilnote. Die Gesamtbewertung ist nicht der Durchschnittswert der Teilnoten. Allerdings verschaffen Ihnen die Teilnoten einen Eindruck, wie leistungsfähig die Komponenten sind, die Ihnen am wichtigsten sind. Außerdem ist das ein wichtiger Faktor bei der Entscheidung, welche Komponenten Sie aufrüsten sollten. Wenn Sie den Computer nicht für Spiele und qualitativ besonders anspruchsvolle 3D-Grafik einsetzen, können Sie einen Computer anschaffen, der leistungsfähige Prozessor-, Arbeitsspeicher- und Festplattenkomponenten hat, aber einen billigeren Grafikadapter. Ein solcher Computer reicht für Ihre Zwecke wahrscheinlich aus, auch wenn er keine hohe Gesamtbewertung erhält.

Dennoch können Sie die Gesamtbewertung zumindest als groben Anhaltspunkt betrachten, wenn Sie auswählen, welche Software auf Ihrem Computer laufen soll. Hat Ihr Computer beispielsweise eine Gesamtbewertung von 3,3, ist es sinnvoll, nur Softwarepakete mit einer Gesamtbewertung von 3 oder niedriger zu kaufen. Interaktive Spiele sind ein gutes Beispiel für Softwarepakete, die einen hohen Windows-Leistungsindex erfordern.

Die Noten reichen von 1,0 bis 7,9. Der Windows-Leistungsindex ist so entworfen, dass er sich an Fortschritte in der Computertechnik anpasst. Wenn Hardwaregeschwindigkeit und -leistung steigen, wird der Notenbereich nach oben erweitert. Die Standards bleiben dabei für jede Indexnote im Großen und Ganzen gleich. In manchen Fällen werden allerdings neue Tests entwickelt, die dazu führen, dass ein Computer schlechtere Noten erhält. Wenn Sie Hardware auf Ihrem Computer ersetzt oder aufgerüstet haben, sollten Sie den Windows-Leistungsindex neu berechnen.

Systemprogramme zum Untersuchen von Prozessen und Diensten

Als IT-Experte haben Sie sicherlich schon den Task-Manager benutzt und von diesem Tool aus den Ressourcenmonitor geöffnet. Möglicherweise kennen Sie aber noch nicht alle Verbesserungen, die der Ressourcenmonitor in Windows 7 bietet. Der Process Explorer ist ein leistungsfähiges Systemtool, das viele der Features von Task-Manager und Ressourcenmonitor vereint. Sie können dieses Tool herunterladen, um Ressourcennutzung, Handles und DLL-Dateien (Dynamic-Link Library) zu untersuchen.

Task-Manager

Falls eine Anwendung nicht mehr reagiert, versucht Windows 7, das Problem zu finden und automatisch zu beseitigen. Wenn das System vollständig abgestürzt zu sein scheint und Windows 7 das Problem nicht gelöst hat, kann der Benutzer die Anwendung aber auch beenden, indem er den Task-Manager öffnet und die Registerkarte *Anwendungen* anklickt.

Die Registerkarte *Leistung* im Task-Manager liefert Details darüber, wie stark ein Computer die Systemressourcen auslastet, zum Beispiel RAM und CPU. Wie Sie in Abbildung 13.13 sehen, enthält die Registerkarte *Leistung* vier Diagramme. Die beiden oberen zeigen die CPU-Auslastung in Prozent, einmal als aktuellen Wert und einmal als Verlauf über die letzten Minuten. Eine hohe Auslastung über längere Zeit deutet darauf hin, dass Programme oder Prozesse eine Menge CPU-Ressourcen benötigen. Das kann sich auf die Computerleistung auswirken. Falls der Prozentsatz eingefroren zu sein scheint oder nahe bei 100 Prozent liegt,

kann es sein, dass ein Programm nicht mehr reagiert. Wenn das Verlaufsdiagramm der CPU-Auslastung unterteilt ist, hat der Computer entweder mehrere CPUs, eine einzige Dual-Core-CPU oder beides.

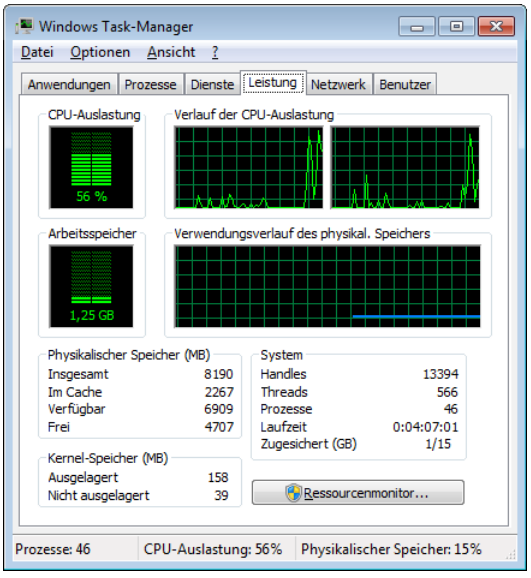


Abbildung 13.13 Registerkarte *Leistung* im Task-Manager

Falls die Prozessorauslastung konstant hoch ist (etwa 80 Prozent oder höher über einen längeren Zeitraum), sollten Sie in Betracht ziehen, einen zweiten Prozessor einzubauen oder den aktuellen Prozessor zu ersetzen. Das gilt auch dann, wenn die Teilbewertung des Windows-Leistungsindex den Prozessor nicht als Leistungsengpass identifiziert. Bevor Sie aber so weit gehen, lohnt es sich, die Prozessorauslastungsdaten mit der Leistungsüberwachung über einen gewissen Zeitraum aufzuzeichnen, statt sich auf Momentaufnahmen zu verlassen, die der Task-Manager geliefert hat.

Die beiden nächsten Diagramme zeigen an, wie viel RAM verwendet wird, einmal als aktuellen Wert und einmal als Verlauf über die letzten Minuten. Unten im Task-Manager-Fenster wird aufgelistet, wie viel Prozent des Speichers benutzt werden. Falls die Speicherauslastung konstant hoch erscheint oder die Leistung Ihres Computers deutlich bremst, sollten Sie versuchen, die Zahl der gleichzeitig geöffneten Programme zu verringern. (Beziehungsweise: Raten Sie den Benutzern, für die Sie Support leisten, alle Anwendungen zu schließen, die sie momentan nicht verwenden.) Falls das Problem weiterhin besteht, müssen Sie unter Umständen mehr RAM installieren oder ReadyBoost aktivieren.

Drei Tabellen unter den Diagrammen listen verschiedene Details über Speicher- und Ressourcenauslastung auf. In der Tabelle *Physikalischer Speicher (MB)* sehen Sie unter *Insgesamt* die Menge des im Computer installierten RAMs. *Im Cache* ist die Menge des Hardwarespeichers, der gerade für Systemressourcen genutzt wird, und *Frei* ist die Speichermenge, die momentan nicht benutzt wird und zur Verfügung steht.

In der Tabelle *Kernel-Speicher (MB)* ist *Insgesamt* die Menge des Speichers, der vom Windows-Kern benutzt wird (der sogenannte Kernel). *Ausgelagert* gibt an, wie viel virtuellen

Arbeitsspeicher der Kernel verwendet. Und *Nicht ausgelagert* ist die RAM-Menge, die vom Kernel benutzt wird.

Die Tabelle *System* hat fünf Felder: *Handles*, *Threads*, *Prozesse*, *Laufzeit* und *Auslagerungsdatei*. Handles sind Zeiger, die auf Systemelemente verweisen. Dazu gehören (unter anderem) Dateien, Registrierungsschlüssel, Ereignisse oder Verzeichnisse. Lektion 2, »Konfigurieren von Leistungseinstellungen«, beschreibt die Konfiguration der Auslagerungsdatei.

Falls Sie mehr Informationen über die Auslastung von Speicher- und CPU-Ressourcen benötigen, können Sie auf die Schaltfläche *Ressourcenmonitor* klicken. Daraufhin wird der Ressourcenmonitor geöffnet, der weiter unten in dieser Lektion beschrieben wird. Sie benötigen erhöhte Privilegien, um auf den Ressourcenmonitor zugreifen zu können.

Sie können feststellen, wie viel Speicher ein einzelner Prozess benutzt, indem Sie im Task-Manager die Registerkarte *Prozesse* anklicken. Wie Sie in Abbildung 13.14 sehen, wird in der Standardeinstellung die Spalte *Arbeitsspeicher (privater Arbeitssatz)* angezeigt. Ein privater Arbeitssatz gibt an, wie viel Speicher, auf den keine anderen Prozesse zugreifen dürfen, ein Prozess verwendet. Diese Information kann nützlich sein, um eine Anwendung zu identifizieren, die »Speicherlecks« verursacht, das heißt eine Anwendung, die immer mehr Speicherressourcen verbraucht und den Speicher nicht wieder freigibt, wenn sie ihn nicht mehr benötigt.

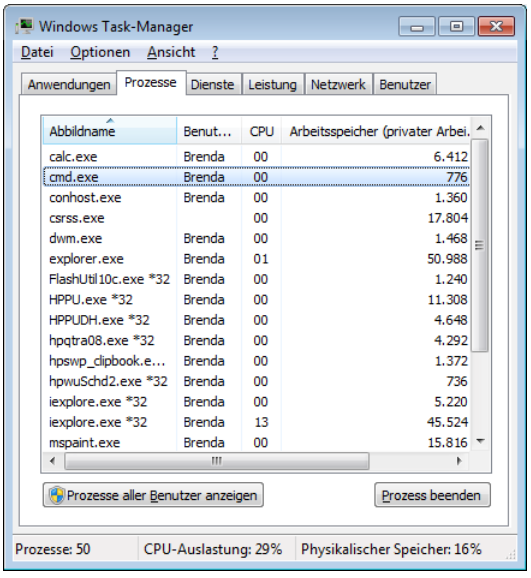

Windows Task-Manager
Datei Optionen Ansicht ?
Anwendungen Prozesse Dienste Leistung Netzwerk Benutzer
Abbildname Benut... CPU Arbeitsspeicher (privater Arbei.
calc.exe Brenda 00 6.412
cmd.exe Brenda 00 776
conhost.exe Brenda 00 1.360
csrss.exe 00 17.804
dwm.exe Brenda 00 1.468
explorer.exe Brenda 01 50.988
FlashUtil10c.exe *32 Brenda 00 1.240
HPPU.exe *32 Brenda 00 11.308
HPPUDH.exe *32 Brenda 00 4.648
hpqtra08.exe *32 Brenda 00 4.292
hpswp_clipbook.e... Brenda 00 1.372
hpwuSchd2.exe *32 Brenda 00 736
iexplore.exe *32 Brenda 00 5.220
iexplore.exe *32 Brenda 13 45.524
mspaint.exe Brenda 00 15.816
Prozesse aller Benutzer anzeigen
Prozess beenden
Prozesse: 50 CPU-Auslastung: 29% Physikalischer Speicher: 16%

Abbildung 13.14 Registerkarte *Prozesse* im Task-Manager

Sie können im Menü *Ansicht* auf *Spalten auswählen* klicken und dann einen Arbeitsspeicherwert auswählen, um andere Details zur Speicherauslastung auf der Registerkarte *Prozesse* anzuzeigen. Sie können auf der Registerkarte *Prozesse* des Task-Managers einen Prozess beenden, eine Prozesshierarchie beenden (den Prozess selbst und alle Prozesse, von denen er abhängt) und die Priorität eines Prozesses verändern. Um die Priorität eines Prozesses zu ändern, klicken Sie mit der rechten Maustaste auf den Prozess und wählen den Befehl *Priorität festlegen*. Zur Auswahl stehen *Echtzeit*, *Hoch*, *Höher als normal*, *Normal*, *Niedriger als normal* und *Niedrig*.

Die Registerkarte *Dienste* des Task-Managers zeigt an, welche Dienste laufen und welche angehalten wurden. Sie können einen Dienst starten oder beenden und zu einem Prozess wechseln, der vom ausgewählten Dienst abhängt. Falls Sie mehr Details oder mehr Steuerungsmöglichkeiten über die Dienste eines Computers erhalten wollen, können Sie auf die Schaltfläche *Dienste* klicken, um die Konsole *Dienste* zu öffnen. Dafür benötigen Sie erhöhte Privilegien.

Auf der Registerkarte *Netzwerk* des Task-Managers können Sie sich die Netzwerkauslastung ansehen. Die Registerkarte *Benutzer* zeigt an, welche Benutzer mit dem Computer verbunden sind. Außerdem können Sie hier die Verbindung zu einem Benutzer trennen. Die Registerkarte *Anwendungen* listet die laufenden Anwendungen auf. Wie bereits erwähnt, können Sie hier eine abgestürzte Anwendung schließen.

Schnelltest

- Sie wollen die Priorität eines Prozesses auf einem Computer ändern. Wie gehen Sie vor?

Antwort zum Schnelltest

- Öffnen Sie den Task-Manager. Klicken Sie auf der Registerkarte *Prozesse* mit der rechten Maustaste auf den Prozess. Öffnen Sie das Untermenü *Priorität festlegen*. Hier können Sie zwischen *Echtzeit*, *Hoch*, *Höher als normal*, *Normal*, *Niedriger als normal* und *Niedrig* wählen.

Ressourcenmonitor

Windows 7 stellt eine verbesserte Version des Ressourcenmonitors zur Verfügung. Im Ressourcenmonitor von Windows 7 können Sie sich Informationen über die Auslastung von Hardware- und Softwareressourcen in Echtzeit ansehen. Sie können die Ergebnisse nach den Prozessen oder Diensten filtern, die Sie überwachen wollen. Und Sie können direkt im Ressourcenmonitor Dienste und Prozesse starten, beenden, anhalten und fortsetzen oder Anwendungen analysieren, die nicht mehr reagieren. Sie öffnen den Ressourcenmonitor auf der Registerkarte *Prozesse* des Task-Managers oder durch Eingabe von **resmon** im Suchfeld des Startmenüs.

Der Ressourcenmonitor startet immer an derselben Position und mit denselben Anzeigeeinstellungen wie in der letzten Sitzung. Sie können Ihre Anzeigeeinstellungen jederzeit sichern und später die Konfigurationsdatei öffnen, um die gespeicherten Einstellungen zu verwenden. Die ausgewählten Filter werden allerdings zusammen mit den Konfigurationseinstellungen gespeichert.

Der Ressourcenmonitor hat fünf Registerkarten: *Übersicht*, *CPU*, *Arbeitsspeicher*, *Datenträger* und *Netzwerk*. Die Registerkarte *Übersicht* (Abbildung 13.15) zeigt grundlegende Informationen zur Auslastung von Systemressourcen an. Die anderen Registerkarten liefern ausführlichere Informationen über die einzelnen Ressourcen. Wenn Sie die Ergebnisse auf einer Registerkarte filtern, werden auch auf den anderen Registerkarten nur die Ressourcen angezeigt, die von den ausgewählten Prozessen oder Diensten benutzt werden. Gefilterte Ergebnisse werden durch eine orangefarbene Leiste unter der Titelzeile jeder Tabelle hervorgehoben.

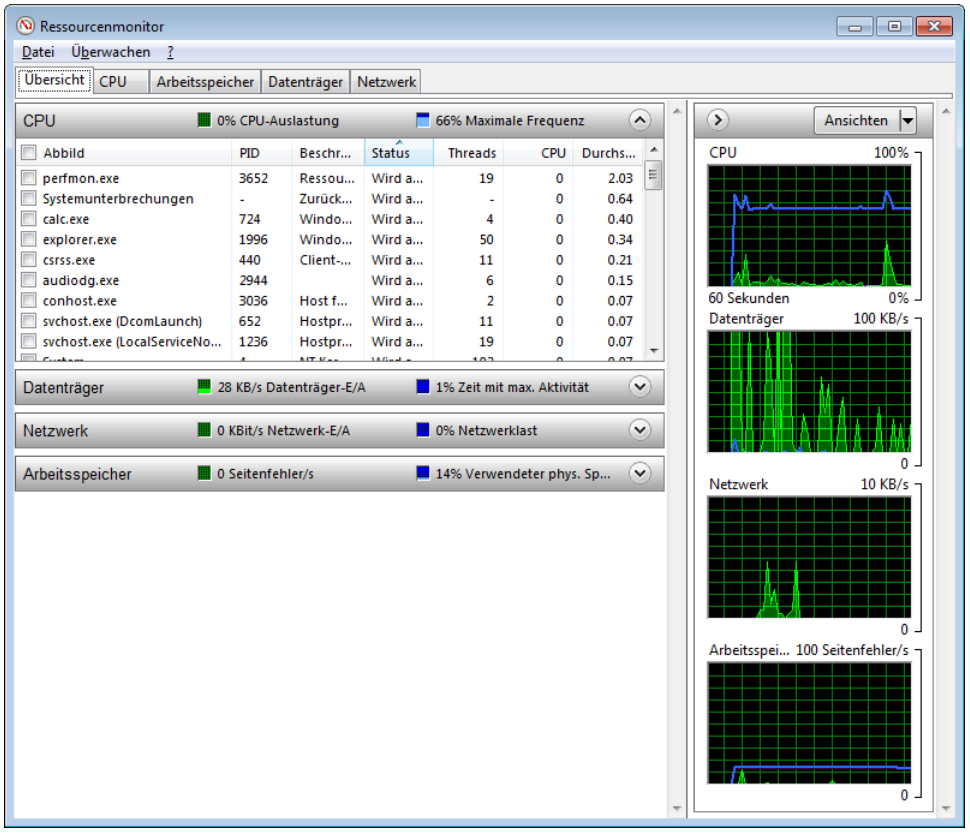

Ressourcenmonitor
Datei Überwachen ?
Übersicht CPU Arbeitsspeicher Datenträger Netzwerk
CPU 0% CPU-Auslastung 66% Maximale Frequenz
Abbild PID Beschr... Status Threads CPU Durchs...
perfmon.exe 3652 Ressou... Wird a... 19 0 2.03
Systemunterbrechungen - Zurück... Wird a... - 0 0.64
calc.exe 724 Windo... Wird a... 4 0 0.40
explorer.exe 1996 Windo... Wird a... 50 0 0.34
csrss.exe 440 Client-... Wird a... 11 0 0.21
audiodg.exe 2944 Wird a... 6 0 0.15
conhost.exe 3036 Host f... Wird a... 2 0 0.07
svchost.exe (DcomLaunch) 652 Hostpr... Wird a... 11 0 0.07
svchost.exe (LocalServiceNo... 1236 Hostpr... Wird a... 19 0 0.07
Datenträger 28 KB/s Datenträger-E/A 1% Zeit mit max. Aktivität
Netzwerk 0 KBit/s Netzwerk-E/A 0% Netzwerklast
Arbeitsspeicher 0 Seitenfehler/s 14% Verwendeter phys. Sp...
Ansichten
CPU 100%
60 Sekunden 0%
Datenträger 100 KB/s
0
Netzwerk 10 KB/s
0
Arbeitsspei... 100 Seitenfehler/s
0

Abbildung 13.15 Die Registerkarte *Übersicht* im Ressourcenmonitor

Jede Registerkarte im Ressourcenmonitor enthält mehrere Tabellen, die ausführliche Informationen über die jeweilige Ressource liefern. Die erste angezeigte Tabelle ist immer die Schlüsseltabelle. Sie enthält eine vollständige Liste aller Prozesse, die Ressourcen des Typs benutzen, der auf der Registerkarte angezeigt wird. Beispielsweise enthält die Schlüsseltabelle auf der Registerkarte *Übersicht* eine vollständige Liste aller Prozesse, die auf dem System laufen.

Sie können die detaillierten Daten in anderen Tabellen als der Schlüsseltabelle filtern, indem Sie einen oder mehrere Prozesse oder Dienste auswählen. Aktivieren Sie dazu in der Schlüsseltabelle neben jedem Prozess oder Dienst, den Sie untersuchen wollen, das zugehörige Kontrollkästchen. Sie beenden die Filterung nach einem einzelnen Prozess oder Dienst wieder, indem Sie das entsprechende Kontrollkästchen deaktivieren. Wenn Sie die Filterung insgesamt abschalten wollen, brauchen Sie nur das Kontrollkästchen *Abbild* in der Schlüsseltabelle zu deaktivieren. Wenn Sie gefilterte Ergebnisse angezeigt bekommen, werden die Ressourcen, die von den ausgewählten Prozesse oder Diensten benutzt werden, in den Diagrammen als orange Linien angezeigt.

Sie können die Größe der Diagramme ändern, indem Sie in der Dropdownliste *Ansichten* einen anderen Eintrag auswählen. Mit dem Pfeilsymbol oben in einem Fensterabschnitt können Sie das zugehörige Diagramm ganz ausblenden. Wenn Sie sich die Definitionen der

Daten ansehen wollen, die in den Tabellen angezeigt werden, setzen Sie den Mauszeiger auf den Kopf der Spalte, über die Sie mehr erfahren wollen.

Wollen Sie zum Beispiel herausfinden, mit welcher Netzwerkadresse ein Prozess verbunden ist, öffnen Sie die Registerkarte *Netzwerk* und klicken auf die Titelzeile *TCP-Verbindungen*, um die Tabelle aufzuklappen. Suchen Sie den Prozess, dessen Netzwerkverbindung Sie analysieren wollen. Nun sehen Sie in den Spalten *Remoteadresse* und *Remoteport*, mit welcher Netzwerkadresse und welchem Port der Prozess verbunden ist. Abbildung 13.16 zeigt den Prozess System, der momentan mit den IPv4-Adressen 192.168.123.138 und 192.168.123.176 verbunden ist, jeweils auf Port 445.

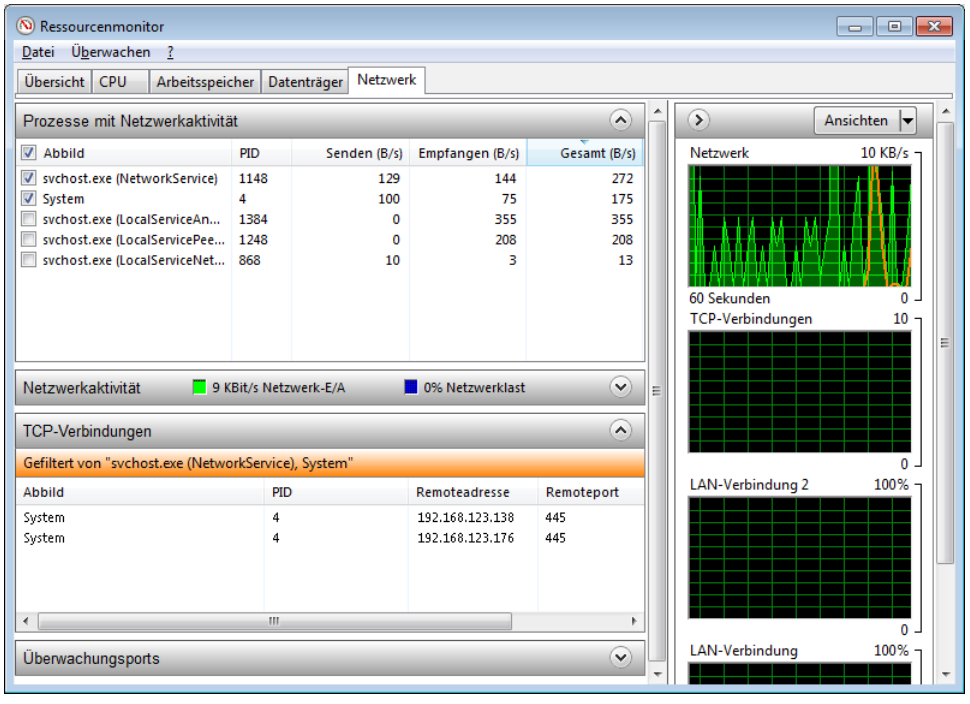


Abbildung 13.16 Ermitteln, mit welchen Netzwerkadressen ein Prozess verbunden ist

Auf der Registerkarte *Arbeitsspeicher* (Abbildung 13.17) sehen Sie, wie viel Arbeitsspeicher von den Programmen benutzt wird. Der verfügbare Arbeitsspeicher ist die Summe aus Standby- und freiem Arbeitsspeicher. Zum freien Arbeitsspeicher gehört auch Nullseitenspeicher.

Der Ressourcenmonitor zeigt Echtzeitinformationen über alle Prozesse an, die auf Ihrem System laufen. Wenn Sie nur die Daten zu ausgewählten Prozessen sehen wollen, können Sie die ausführlichen Ergebnisse filtern, indem Sie in einer beliebigen Registerkarte die Kontrollkästchen neben den Namen der Prozesse aktivieren, die Sie überwachen wollen. So ausgewählte Prozesse werden an das obere Ende der Spalte *Abbild* verschoben. Sobald Sie mindestens einen Prozess zum Filtern ausgewählt werden, enthalten die Tabellen *Zugeordnete Handles* und *Zugeordnete Tabellen* auf der Registerkarte *CPU* die Daten zu den ausgewählten Elementen. Tabellen, die nur gefilterte Ergebnisse enthalten, werden durch eine orangefarbene Informationsleiste unter der Titelzeile der Tabelle kenntlich gemacht.

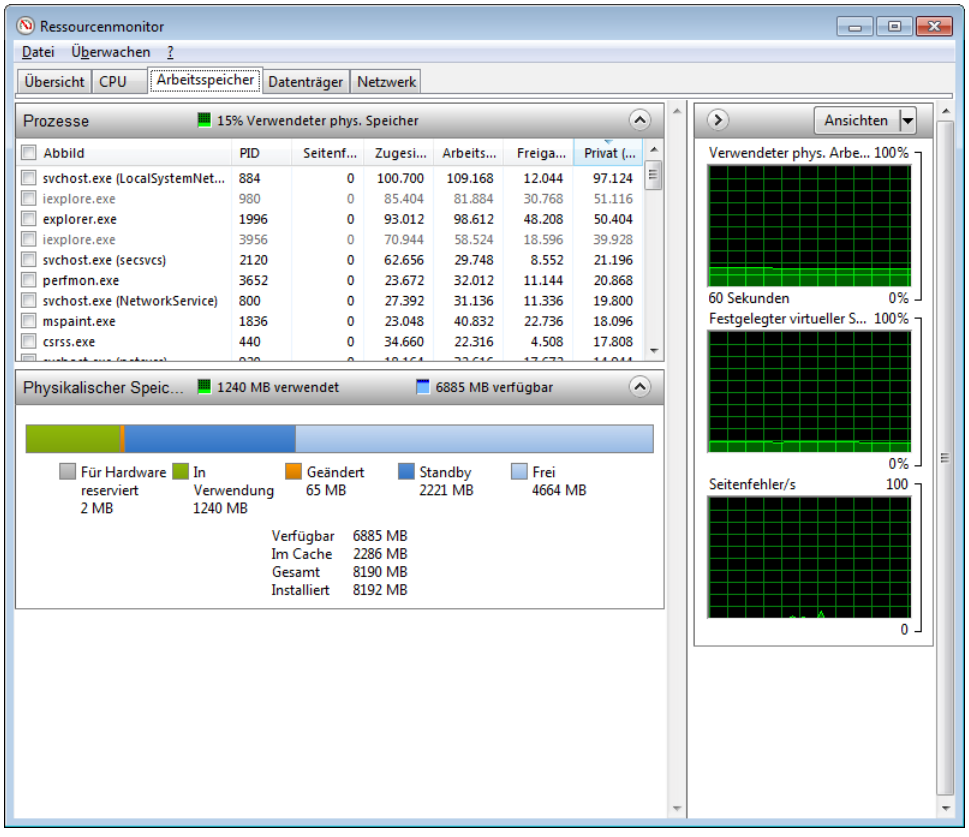

Ressourcenmonitor
Datei Überwachen ?
Übersicht CPU Arbeitsspeicher Datenträger Netzwerk
Prozesse
15% Verwendeter phys. Speicher
Abbild PID Seitenf... Zugesi... Arbeits... Freiga... Privat (...
svchost.exe (LocalSystemNet... 884 0 100.700 109.168 12.044 97.124
iexplore.exe 980 0 85.404 81.884 30.768 51.116
explorer.exe 1996 0 93.012 98.612 48.208 50.404
iexplore.exe 3956 0 70.944 58.524 18.596 39.928
svchost.exe (secsvcs) 2120 0 62.656 29.748 8.552 21.196
perfmon.exe 3652 0 23.672 32.012 11.144 20.868
svchost.exe (NetworkService) 800 0 27.392 31.136 11.336 19.800
mspaint.exe 1836 0 23.048 40.832 22.736 18.096
csrss.exe 440 0 34.660 22.316 4.508 17.808
Physikalischer Speic...
1240 MB verwendet
6885 MB verfügbar
Für Hardware reserviert 2 MB
In Verwendung 1240 MB
Geändert 65 MB
Standby 2221 MB
Frei 4664 MB
Verfügbar 6885 MB
Im Cache 2286 MB
Gesamt 8190 MB
Installiert 8192 MB
Ansichten
Verwendeter phys. Arbe... 100%
60 Sekunden 0%
Festgelegter virtueller S... 100%
0%
Seitenfehler/s 100
0

Abbildung 13.17 Die Registerkarte *Arbeitsspeicher* im Ressourcenmonitor

Sie können im Ressourcenmonitor Prozesse anhalten oder beenden und Dienste starten, beenden oder neu starten. Sie sollten einen Prozess nur dann im Ressourcenmonitor beenden, wenn es Ihnen nicht gelingt, das Programm mit normalen Mitteln zu schließen. Ist ein offenes Programm mit dem Prozess verbunden, schließt es sich sofort und Sie verlieren alle Daten, die nicht vorher gespeichert wurden. Wenn Sie einen Systemprozess beenden, kann das sogar dazu führen, dass das System instabil wird oder Daten verliert.

Sie beenden einen Prozess, indem Sie auf irgendeiner Registerkarte des Ressourcenmonitors in der Spalte *Abbild* der Schlüsseltabelle mit der rechten Maustaste auf den Namen der ausführbaren Datei des Prozesses klicken, den Sie beenden wollen, und den Befehl *Prozess beenden* wählen. Sie können auch alle Prozesse beenden, die vom ausgewählten Prozess abhängen, indem Sie stattdessen *Prozessstruktur beenden* wählen. Sie setzen einen Prozess fort, indem Sie mit der rechten Maustaste auf den Namen der ausführbaren Datei des Programms klicken, das Sie fortsetzen wollen, und den Befehl *Vorgang fortsetzen* wählen.

Sie können einen Dienst im Ressourcenmonitor beenden, starten oder neu starten, indem Sie die Registerkarte *CPU* öffnen und auf die Titelzeile *Dienste* klicken, um die entsprechende Tabelle aufzuklappen. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf den Dienst, den Sie bearbeiten wollen, und wählen Sie den Befehl *Dienst beenden*, *Dienst starten* oder *Dienst neu starten*.

Anwendungen, die nicht mehr reagieren, warten unter Umständen darauf, dass andere Prozesse beendet werden oder dass bestimmte Systemressourcen frei werden. Sie können sich im Ressourcenmonitor die Warteschlange der Prozesse ansehen und Prozesse beenden, die verhindern, dass ein Programm funktioniert.

Ein Prozess, der nicht reagiert, wird in der Tabelle *CPU* der Registerkarte *Übersicht* sowie in der Tabelle *Prozesse* der Registerkarte *CPU* als roter Eintrag markiert. Sie können sich die Prozesswarteschlange ansehen, indem Sie auf irgendeiner Registerkarte des Ressourcenmonitors in der Spalte *Abbild* der Schlüsseltabelle mit der rechten Maustaste auf den Namen der ausführbaren Datei des Prozesses klicken, den Sie untersuchen wollen, und den Befehl *Warteschlange analysieren* wählen.

Wenn der Prozess normal läuft und nicht auf andere Prozesse wartet, werden keine Informationen zur Warteschlange angezeigt. Wartet der Prozess dagegen auf einen anderen Prozess, wird eine Struktur angezeigt, die darstellt, welche Abhängigkeiten von anderen Prozessen bestehen. Wenn eine Warteschlangenstruktur angezeigt wird, können Sie Prozesse in der Strukturansicht beenden, indem Sie das Kontrollkästchen neben dem Prozessnamen aktivieren und auf *Prozess beenden* klicken. Handles sind (wie bereits weiter oben in diesem Abschnitt erklärt) Zeiger, die auf Systemelemente verweisen. Das sind (unter anderem) Dateien, Registrierungsschlüssel, Ereignisse oder Verzeichnisse. Module sind Hilfsdateien oder -programme. Dies sind unter anderem DLL-Dateien.

Sie können sich im Ressourcenmonitor alle Handles und Module ansehen, die mit einem Prozess verknüpft sind, indem Sie in der Spalte *Abbild* auf der Registerkarte *CPU* das Kontrollkästchen neben dem Namen des Prozesses aktivieren, dessen Handles und Module Sie untersuchen wollen. Ausgewählte Prozesse werden an den Anfang der Tabelle verschoben. Klicken Sie auf die Titelzeilen der Tabellen *Zugeordnete Handles* und *Zugeordnete Module*, um sie zu erweitern. Eine orangefarbene Leiste unter der Titelzeile jeder Tabelle zeigt die ausgewählten Prozesse. Sehen Sie sich die Ergebnisse in den Detailtabellen an.

Wenn Sie herausfinden wollen, welche Prozesse ein bestimmtes Handle benutzen, können Sie in der Titelzeile der Tabelle *Zugeordnete Handles* auf *Handles durchsuchen* klicken. Geben Sie den Namen des Handles ein, das Sie untersuchen wollen, und klicken Sie auf die Suchschaltfläche. Wenn Sie beispielsweise nach *c:\windows* suchen, werden alle Handles zurückgegeben, die *c:\windows* im Handlenamen tragen. Bei der Suchzeichenfolge wird nicht zwischen Groß- und Kleinschreibung unterschieden, und es sind keine Platzhalterzeichen erlaubt.

Process Explorer

Der Process Explorer ist nicht Teil von Windows 7, aber Sie können ihn von *http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx* herunterladen. Entpacken Sie das Archiv in einen Ordner (etwa *C:\ProcessExplorer*) und starten Sie das Tool, indem Sie im Suchfeld des Startmenüs **c:\processexplorer\procexp.exe** eingeben. Der Process Explorer verrät Ihnen, welches Programm eine bestimmte Datei oder ein Verzeichnis geöffnet hat, und zeigt Informationen darüber an, welche Handles und DLLs die Prozesse geöffnet oder geladen haben. Sie können den Process Explorer oder den Ressourcenmonitor verwenden, um festzustellen, welche Anwendungen für Aktivitäten auf Ihrer Festplatte verantwortlich sind. So können Sie unter anderem ermitteln, auf welche Dateien und Ordner zugegriffen wird.

Nach dem Start zeigt der Process Explorer eine Liste der momentan aktiven Prozesse an (Abbildung 13.18). Sie können den unteren Fensterabschnitt an- und ausschalten und aus-

wählen, ob Sie Handles oder DLLs auflisten wollen. Im Handlemodus bekommen Sie angezeigt, welche Handles der Prozess, der im oberen Fensterabschnitt ausgewählt ist, gerade geöffnet hat. Die Suchfunktionen des Process Explorers finden heraus, welche Prozesse bestimmte Handles geöffnet beziehungsweise DLLs geladen haben.

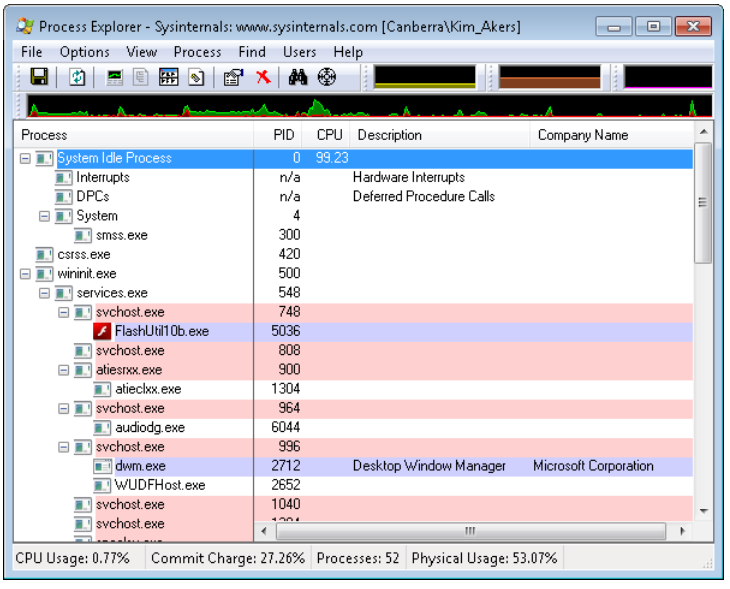


Abbildung 13.18 Startseite des Process Explorers



Weitere Informationen **Fortgeschrittene Systemtools und Befehlszeilenprogramme**

Weitere Informationen über fortgeschrittene Systemtools für Windows und die entsprechenden Befehlszeilenprogramme finden Sie unter *http://technet.microsoft.com/de-de/sysinternals/default.aspx*.

Der Process Explorer enthält eine Symbolleiste und Minidiagramme für CPU, Arbeitsspeicher und E/A-Verlauf. Die Minidiagramme zeigen den Verlauf der Systemaktivitäten. Wenn Sie die Maus über einen Punkt des Diagramms stellen, werden die zugehörige Uhrzeit und die Prozessinformationen angezeigt. Beispielsweise zeigt das Tooltip für das CPU-Minidiagramm den Prozess an, der die CPU am stärksten belastet hat. Wenn Sie auf eines der Minidiagramme klicken, öffnet sich ein Fenster mit Systeminformationen (Abbildung 13.19). Die Hervorhebung von Veränderungen bei den Werten hilft Ihnen zu erkennen, welche Elemente sich zwischen den Aktualisierungen ändern. Elemente (darunter Prozesse, DLLs und Handles), die enden oder geschlossen werden, werden in roter Farbe angezeigt, neue Elemente in grüner Farbe.

Die Diagramme im Fenster mit den Systeminformationen zeigen den Verlauf der CPU-Auslastung, des zugeordneten virtuellen Arbeitsspeichers und des E/A-Durchsatzes an. Rote Farbe im Diagramm der CPU-Auslastung bedeutet, dass die CPU im Kernelmodus läuft, grüne Farbe steht für die Summe aus Kernelmodus- und Benutzermodusausführung. Wenn der zugeordnete virtuelle Arbeitsspeicher das Limit für den zugeordneten Systemspeicher erreicht, wird das System instabil. Das Zuordnungslimit ist die Summe des (beinahe) ge-

samten physischen Arbeitsspeichers und der Größe aller Auslagerungsdateien. Im E/A-Diagramm stehen die blauen Linien für den gesamten E/A-Verkehr, also die Summe aller E/A-Lese- und Schreiboperationen aller Prozesse zwischen zwei Aktualisierungen. Die rosa Linie zeigt den Schreibverkehr an.

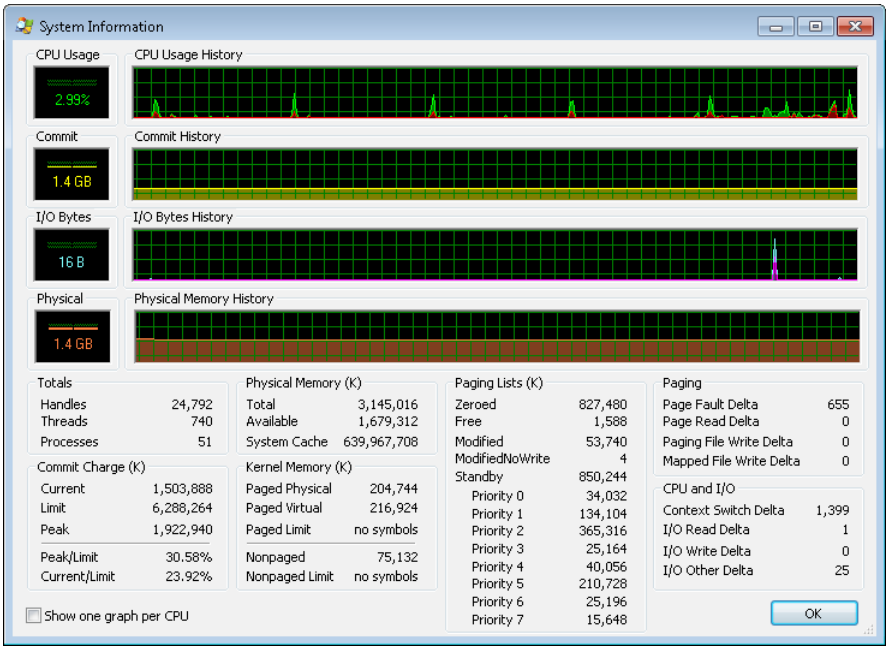


Abbildung 13.19 Systeminformationen im Process Explorer

Sie können die Reihenfolge der Spalten im Process Explorer ändern, indem Sie sie einfach mit der Maus an den neuen Platz ziehen. Um auszuwählen, welche Datenspalten in jeder Ansicht und der Statuszeile angezeigt werden, können Sie im Menü *View* den Befehl *Select Columns* wählen oder mit der rechten Maustaste auf einen Spaltenkopf klicken und den Befehl *Select Columns* wählen. Sie speichern eine Spaltenkonfiguration und die zugehörigen Einstellungen, indem Sie im Menü *View* den Befehl *Save Column Set* wählen.

Im Menü *Options* wählen Sie aus, ob statt des Task-Managers der Process Explorer gestartet werden soll. Außerdem können Sie veranlassen, dass das Fenster des Process Explorers immer im Vordergrund erscheint und immer sichtbar ist. Schließlich können Sie noch festlegen, dass immer nur eine einzige Instanz des Process Explorers geöffnet sein darf.



Hinweis **Der Link *Erweiterte Systemdetails in den Systeminformationen anzeigen***

Der Link *Erweiterte Systemdetails in den Systeminformation anzeigen*, der sichtbar wird, wenn Sie im Dialogfeld *Leistungsinformationen und -tools* auf *Weitere Tools* klicken, zeigt ausführliche Informationen über die Systemkonfiguration an. Dieses Fenster liefert aber keine unmittelbaren Daten zu Leistungsproblemen, es heißt allerdings ganz ähnlich, nämlich *Systeminformationen*. Verwechseln Sie dieses Dialogfeld, das in Windows 7 enthalten ist, nicht mit dem Feature *System Information* im Process Explorer, einem Tool, das Sie herunterladen können.

Protokollieren und Weiterleiten von Ereignissen und Ereignisabonnements

Als erfahrener IT-Experte haben Sie sicherlich schon mit der Ereignisanzeige und mit Ereignisprotokollen gearbeitet. Dieser Abschnitt beschreibt diese Tools daher nur kurz, bevor er Ereignisweiterleitung und Ereignisabonnements vorstellt, mit denen Sie möglicherweise noch nicht vertraut sind.

Details über Ereignisabonnements finden Sie auf der Registerkarte *Abonnements* im Eigenschaftendialogfeld eines Ereignisprotokolls. Die Registerkarte *Allgemein* dieses Dialogfelds enthält Details wie die aktuelle Größe des Protokolls, die Maximalgröße des Protokolls und was getan wird, wenn die Maximalgröße erreicht ist. Am einfachsten starten Sie die Ereignisanzeige, indem Sie im Suchfeld des Startmenüs **eventvwr** eingeben.

Die Ereignisanzeige zeigt Ereignisprotokolle an. Das sind Dateien, die wichtige Ereignisse auf einem Computer aufzeichnen, zum Beispiel wenn sich ein Benutzer anmeldet oder wenn ein Programm einen Fehler verursacht. Sie werden feststellen, dass die Details in den Ereignisprotokollen für die Problembehandlung nützlich sind. Die Ereignisse werden in folgende Kategorien eingeteilt:

- Kritisch
- Fehler
- Warnung
- Informationen

Das Sicherheitsprotokoll enthält zwei weitere Ereigniskategorien, die für Überwachungszwecke benutzt werden: Erfolgsüberwachung und Fehlerüberwachung.

Die Ereignisanzeige zeichnet Informationen in unterschiedlichen Protokollen auf. Windows-Protokolle sind:

- **Anwendung** Speichert Programmereignisse. Ereignisse werden in die Ebenen »Fehler«, »Warnung« oder »Informationen« eingeteilt, abhängig vom Schweregrad des Ereignisses. Die Ebene »Kritisch« wird im Anwendungsprotokoll nicht benutzt.
- **Sicherheit** Speichert sicherheitsrelevante Überwachungsereignisse. Diese Ereignisse können erfolgreiche oder fehlgeschlagene Operationen aufzeichnen. Zum Beispiel zeichnet das Sicherheitsprotokoll eine Erfolgsüberwachung auf, wenn ein Benutzer sich erfolgreich am Computer angemeldet hat.
- **System** Speichert Systemereignisse, die von Windows 7 und den Systemdiensten aufgezeichnet werden. Systemereignisse werden in die Ebenen »Kritisch«, »Fehler«, »Warnung« oder »Informationen« eingeteilt.
- **Weitergeleitete Ereignisse** Speichert Ereignisse, die von anderen Computern weitergeleitet werden.

Benutzerdefinierte Ansichten

Sie können in der Ereignisanzeige benutzerdefinierte Ansichten erstellen, indem Sie im Menü *Aktion* auf *Benutzerdefinierte Ansicht erstellen* klicken und dann die Quellprotokolle oder Ereignisse, Ereignisebene, protokollierte Zeit, Ereignis-ID, Aufgabenkategorie, Schlüsselwörter, Benutzer oder Computer auswählen. Sie werden nur selten alle diese Kriterien angeben, aber mit diesen Einstellungen können Sie Ihre Suche auf die Elemente einschrän-

ken, bei denen Sie ein Problem vermuten. Sie vermeiden also, sehr viele Ereignisse durchsuchen zu müssen. Abbildung 13.20 zeigt die Definition einer benutzerdefinierten Ansicht.

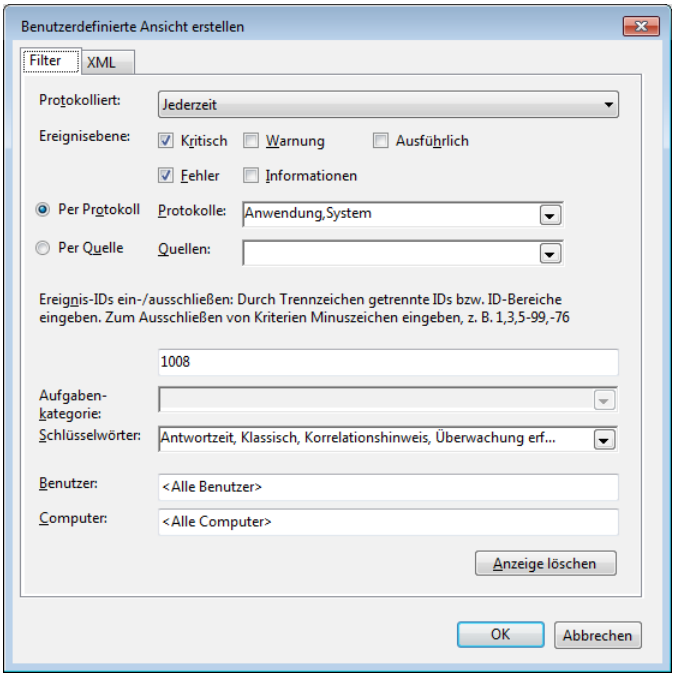


Abbildung 13.20 Erstellen einer benutzerdefinierten Ansicht

Ein Filter ist nicht dauerhaft. Wenn Sie einen Filter einrichten, um sich ausgewählte Informationen in einem Ereignisprotokoll anzusehen, müssen Sie den Filter erneut konfigurieren, wenn Sie diese Daten später wieder sehen wollen. Benutzerdefinierte Ansichten sind dagegen dauerhaft, das bedeutet, dass Sie jedes Mal darauf Zugriff haben, wenn Sie die Ereignisanzeige öffnen. Sie können einen Filter als benutzerdefinierte Ansicht speichern, sodass er dauerhaft wird und Sie ihn nicht jedes Mal neu konfigurieren müssen. Im Menü *Aktion* können Sie auch benutzerdefinierte Ansichten aus anderen Quellen importieren und eine Verbindung zu einem anderen Computer herstellen. Sie brauchen dazu ein Administratorkonto auf diesem Computer.

Anwendungs- und Dienstprotokolle

Die Ereignisanzeige stellt eine Reihe von Anwendungs- und Dienstprotokollen zur Verfügung. Darunter sind Protokolle für Programme, die auf dem Computer laufen, und detaillierte Protokolle mit Informationen über bestimmte Windows-Dienste. Zum Beispiel können folgende Protokolle vorhanden sein:

- Hardwareereignisse
- Internet Explorer
- Key Management Service
- Media Center
- Eine große Zahl von Microsoft Windows-Protokollen

- Microsoft Office-Diagnose
- Microsoft Office-Sitzungen
- Windows PowerShell

Verknüpfen von Aufgaben mit Ereignissen

Manchmal wollen Sie durch E-Mail benachrichtigt werden, falls ein bestimmtes Ereignis auftritt, oder Sie möchten, dass in diesem Fall ein angegebenes Programm gestartet wird – zum Beispiel eines, das eine SMS aussendet. Normalerweise wollen Sie, dass ein Ereignis im Sicherheitsprotokoll diese Aktion auslöst. Das kann zum Beispiel eine fehlgeschlagene Anmeldung oder die erfolgreiche Anmeldung durch einen Benutzer sein, der nicht in der Lage sein sollte, sich an einem bestimmten Computer anzumelden. Sie können diese Funktion implementieren, indem Sie eine Aufgabe mit dem Ereignis verknüpfen, sodass Sie eine Benachrichtigung erhalten.

Öffnen Sie dazu die Ereignisanzeige und navigieren Sie zu dem Protokoll, das ein Ereignis enthält, über das Sie benachrichtigt werden wollen. Normalerweise ist dies das Sicherheitsprotokoll innerhalb der Windows-Protokolle, aber Sie können auch andere Windows-Protokolle oder Anwendungs- und Dienstprotokolle verwenden, wenn Sie möchten. Sie können das Ereignis auswählen und auf *Aktion* klicken, das Ereignis anklicken und in den Abschnitt *Aktionen* wechseln oder mit der rechten Maustaste auf das Ereignis klicken und den Befehl *Aufgabe an dieses Ereignis anfügen* wählen.

Daraufhin wird der Assistent für das Erstellen einfacher Aufgaben geöffnet. Geben Sie einen Namen und eine Beschreibung für die Aufgabe ein und klicken Sie dann auf *Weiter*. Die nächste Seite fasst das Ereignis zusammen und Sie können sich vergewissern, dass Sie das richtige Ereignis ausgewählt haben, bevor Sie auf *Weiter* klicken. Auf der nächsten Seite haben Sie die Möglichkeit, ein Programm zu starten, eine E-Mail zu senden oder eine Meldung anzuzeigen. Nachdem Sie die gewünschte Option ausgewählt und auf *Weiter* geklickt haben, müssen Sie die Aufgabe konfigurieren. Wenn Sie zum Beispiel eine E-Mail senden wollen, geben Sie Absenderadresse, Zieladresse, Betreffzeile, Aufgabe, Anhang (sofern nötig) und Namen des SMTP-Servers (Simple Mail Transfer Protocol) ein. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Kombinieren der Netzwerkdiagnose mit der Ereignisanzeige

Wenn Sie die Windows-Netzwerkdiagnose ausführen, wie in Kapitel 6 beschrieben, werden alle gefundenen Probleme zusammen mit den Lösungen im Dialogfeld *Netzwerkdiagnose* angezeigt. Stehen allerdings detailliertere Informationen über das Problem und potenzielle Lösungen zur Verfügung, speichert Windows 7 sie in einem oder mehreren Ereignisprotokollen. Als Netzwerkadministrator oder Supportmitarbeiter verwenden Sie die Informationen in den Ereignisprotokollen, um Verbindungsprobleme zu analysieren oder die Ergebnisse zu interpretieren.

Sie können nach Netzwerkdiagnose- und TCP/IP-Ereignissen (Transmission Control Protocol/Internet Protocol) filtern, indem Sie als Ereignisquellen beispielsweise *Tcpip* und *Tcpip-v6* auswählen und Ereignisse aus diesen Quellen in einer benutzerdefinierten Ansicht anzeigen.

Falls die Netzwerkdiagnose ein Problem mit einem Drahtlosnetzwerk findet, speichert sie die Informationen im Ereignisprotokoll entweder als Hilfsklassen- oder als Informationsereignis. Hilfsklassenereignisse bieten eine Zusammenfassung der Diagnoseergebnisse und

wiederholen Informationen, die im Dialogfeld *Netzwerkdiagnose* angezeigt werden. Sie können auch zusätzliche Informationen für die Fehlerbehebung liefern, zum Beispiel Details über die Verbindung, die untersucht wurde, Diagnoseergebnisse und die Fähigkeiten des Drahtlosnetzwerks und des untersuchten Adapters.

Informationsereignisse können unter anderem folgende Informationen umfassen: die untersuchte Verbindung, die Drahtlosnetzwerkeinstellungen auf dem Computer und im Netzwerk, sichtbare Netzwerke und Router oder Zugriffspunkte zum Zeitpunkt der Diagnose, die bevorzugten Drahtlosnetzwerke des Computers, den Verbindungsverlauf und Verbindungsstatistiken, zum Beispiel Paketstatistiken und Roaming-Verlauf. Sie fassen außerdem Verbindungsversuche zusammen, listen ihren Status auf und geben an, welche Phasen der Verbindung fehlgeschlagen sind oder nicht gestartet wurden.

Ereignisweiterleitung und Ereignisabonnements

Mithilfe der *Ereignisweiterleitung* (event forwarding) übertragen Sie alle Ereignisse, die bestimmte Kriterien erfüllen, an einen Verwaltungscomputer (den sogenannten Sammelcomputer). So können Sie die Ereignisse zentral verwalten. Ein einziges *Ereignisprotokoll* auf dem Sammelcomputer enthält wichtige Ereignisse von vielen Computern in Ihrer gesamten Organisation. Sie brauchen keine Verbindung zu den lokalen Ereignisprotokollen auf den verschiedenen Computern mehr herzustellen.

Die Ereignisweiterleitung arbeitet über HTTP (Hypertext Transfer Protocol) oder (wenn Sie aus Sicherheitsgründen eine zusätzliche Verschlüsselungs- und Authentifizierungsschicht brauchen) über HTTPS (Hypertext Transfer Protocol Secure), um Ereignisse von einem Quellcomputer an einen Sammelcomputer zu senden. Weil die Ereignisweiterleitung also dieselben Protokolle benutzt wie Sie beim Surfen im Web, funktioniert sie durch die meisten Firewalls und Proxyserver hindurch. Ereignisweiterleitungsverkehr ist immer verschlüsselt, sowohl bei Verwendung von HTTP als auch von HTTPS.

Um die Ereignisweiterleitung zu nutzen, müssen Sie Quell- und Sammelcomputer konfigurieren. Starten Sie auf beiden Computern die Dienste *Windows-Remoteverwaltung (WS-Verwaltung)* und *Windows-Ereignissammlung*. Konfigurieren Sie auf dem Quellcomputer eine Windows-Firewall-Ausnahme für das Protokoll HTTP. Unter Umständen müssen Sie auch eine Windows-Firewall-Ausnahme auf dem Sammelcomputer einrichten; das hängt davon ab, welche Auslieferungsoptimierungstechnik Sie verwenden.

Sie können sammlungsinitiierte (collector-initiated) oder quellinitiierte (source-initiated) Abonnements konfigurieren. Bei sammlungsinitiierten Abonnements ruft der Sammelcomputer die Ereignisse von dem Computer ab, auf dem das Ereignis auftritt. Ein sammlungsinitiiertes Abonnement verwenden Sie, wenn Sie eine überschaubare Zahl von Quellcomputern haben, die alle bereits bekannt sind. Bei dieser Art Abonnement konfigurieren Sie jeden Computer von Hand.

Abonnements

Bei einem quellinitiierten Abonnement (auch als *quellcomputerinitiiertes Abonnement* bezeichnet) sendet der Computer, auf dem ein Ereignis auftritt (der Quellcomputer), das Ereignis an den Sammelcomputer. Ein quellinitiiertes Abonnement eignet sich, wenn Sie sehr viele Quellcomputer haben und diese Computer mithilfe von Gruppenrichtlinien konfigurieren.

Bei einem quellinitiierten Abonnement können Sie weitere Quellcomputer hinzufügen, auch nachdem das Abonnement eingerichtet ist. Sie brauchen also nicht schon vorher genau zu

wissen, welche Computer in Ihrem Netzwerk als Quellcomputer agieren. Dagegen ruft bei sammlungsinitiierten Abonnements der Sammelcomputer die Ereignisse von Quellcomputern ab. Sammlungsinitiierte Abonnements werden meist in kleinen Netzwerken benutzt. Bei quellinitiierten Abonnements leiten die Quellcomputer ihre Ereignisse an den Sammelcomputer weiter. Solche quellinitiierten Abonnements eignen sich besser für große Unternehmensnetzwerke.

Ein Sammelcomputer muss unter Windows Server 2008 R2, Windows Server 2008, Windows 7, Windows Vista oder Windows Server 2003 R2 laufen. Quellcomputer müssen unter Windows XP mit SP2, Windows Server 2003 mit SP1 oder SP2, Windows Server 2003 R2, Windows Vista, Windows 7, Windows Server 2008 oder Windows Server 2008 R2 laufen.



Hinweis Weiterleitungscomputer

Viele Artikel zu diesem Thema verwenden statt *Quellcomputer* den Befehl *Weiterleitungscomputer* (forwarding computer). Diese Bezeichnung ist nicht immer ganz richtig. Bei sammlungsinitiierten Abonnements ruft der Sammelcomputer Ereignisse vom Quellcomputer ab. Der Quellcomputer leitet also keine Ereignisse weiter. Nur bei quellinitiierten Abonnements leitet der Quellcomputer selbst Ereignisse weiter, sodass die Bezeichnung Weiterleitungscomputer sinnvoll ist. Um Missverständnisse zu vermeiden, wird in diesem Kapitel durchgehend die Bezeichnung *Quellcomputer* verwendet, nicht *Weiterleitungscomputer*.

Bei einem sammlungsinitiierten Abonnement konfigurieren Sie zuerst von Hand einen oder mehrere Quellcomputer sowie den Sammelcomputer. Anschließend erstellen Sie ein *Ereignisabonnement*, um festzulegen, welche Ereignisse übertragen werden sollen.

Konfigurieren eines sammlungsinitiierten Abonnements

Sie konfigurieren einen Windows 7-Quellcomputer, damit ein Sammelcomputer seine Ereignisse abrufen kann. Öffnen Sie dazu eine Eingabeaufforderung mit erhöhten Rechten und konfigurieren Sie den Dienst *Windows-Remoteverwaltung* mit dem Befehlszeilentool Winrm:

```
winrm quickconfig
```

Sie können diesen Befehl auch als `winrm qc` abkürzen. Windows zeigt eine Meldung an, die der in Abbildung 13.21 ähnelt. Welche Änderungen durchgeführt werden müssen, hängt davon ab, wie das Betriebssystem konfiguriert ist. Geben Sie J ein, um die Änderungen vorzunehmen. Wenn eine Ihrer Netzwerkschnittstellen den Typ »öffentlich« hat, müssen Sie sie auf »privat« setzen, damit dieser Befehl funktioniert.

Fügen Sie nun das Computerkonto des Sammelcomputers auf dem Quellcomputer zur lokalen Gruppe *Ereignisprotokollleser* oder *Administratoren* hinzu. Das können Sie im MMC-Snap-In *Lokale Benutzer und Gruppen* erledigen oder mit einem `net`-Befehl in einer Eingabeaufforderung mit erhöhten Rechten.

Sie haben die Wahl, das Konto des Sammelcomputers auf dem Quellcomputer entweder zur lokalen Gruppe *Administratoren* oder zur Gruppe *Ereignisprotokollleser* hinzuzufügen. Wenn es nicht nötig ist, dass der Sammelcomputer Ereignisse im Sicherheitsereignisprotokoll abruft, wird empfohlen, die Gruppe *Ereignisprotokollleser* zu verwenden. Wollen Sie dagegen Daten aus dem Sicherheitsereignisprotokoll übertragen, müssen Sie die lokale Gruppe *Administratoren* nehmen.

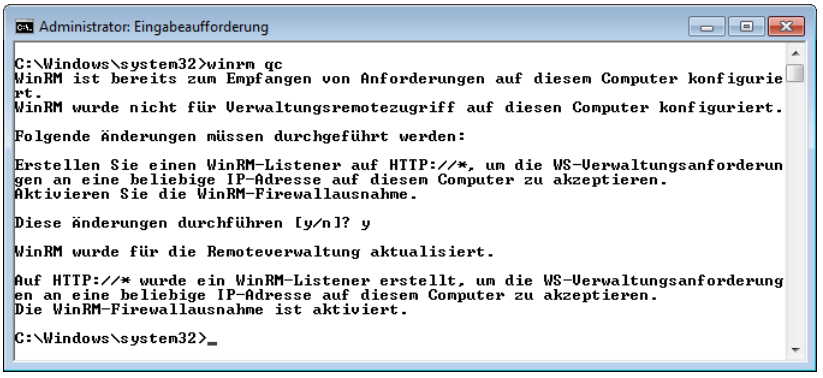

Administrator: Eingabeaufforderung
C:\Windows\system32>winrm qc
WinRM ist bereits zum Empfangen von Anforderungen auf diesem Computer konfiguriert.
WinRM wurde nicht für Verwaltungsremotezugriff auf diesen Computer konfiguriert.
Folgende Änderungen müssen durchgeführt werden:
Erstellen Sie einen WinRM-Listener auf HTTP://*, um die WS-Verwaltungsanforderungen an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Aktivieren Sie die WinRM-Firewallausnahme.
Diese Änderungen durchführen [y/n]? y
WinRM wurde für die Remoteverwaltung aktualisiert.
Auf HTTP://* wurde ein WinRM-Listener erstellt, um die WS-Verwaltungsanforderungen an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Die WinRM-Firewallausnahme ist aktiviert.
C:\Windows\system32>_

Abbildung 13.21 Konfigurieren des Windows-Remoteverwaltungsdienstes

In der Standardeinstellung ist es im MMC-Snap-In *Lokale Benutzer und Gruppen* nicht möglich, Computerkonten hinzuzufügen. Sie müssen dazu im Dialogfeld *Benutzer, Computer oder Gruppen wählen* auf die Schaltfläche *Objekttypen* klicken und das Kontrollkästchen *Computer* aktivieren. Anschließend können Sie Computerkonten hinzufügen.

Um einen Windows 7-Computer als Sammelcomputer zu konfigurieren, öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und geben den folgenden Befehl ein, um den Dienst *Windows-Ereignissammlung* zu konfigurieren:

```
wecutil qc
```

Wenn Sie die Quell- und Sammelcomputer konfiguriert haben, richten Sie ein Ereignisabonnement ein, indem Sie festlegen, welche Ereignisse der Sammelcomputer abruft und auf welche Ereignisquellen (insbesondere auf welche Quellcomputer) er dabei zugreift.



Prüfungstipp

Verwechseln Sie *Winrm* und *Wecutil* nicht. Winrm wird benutzt, um die Windows-Remoteverwaltung zu konfigurieren; es wird normalerweise auf dem Quellcomputer benutzt. Wecutil konfiguriert den Windows-Ereignissammlungsdienst; es wird normalerweise auf dem Sammelcomputer aufgerufen.

Konfigurieren eines quellinitiierten Abonnements

Quellinitiierte Abonnements werden meist in großen Unternehmensnetzwerken eingesetzt, in denen Sie mit Gruppenrichtlinien viele Quellcomputer auf einmal konfigurieren können. Wenn Sie ein quellinitiiertes Abonnement einrichten, müssen Sie den Sammelcomputer von Hand konfigurieren. Die Quellcomputer können Sie dagegen mithilfe von Gruppenrichtlinien konfigurieren. Sobald Sammelcomputer und Quellcomputer konfiguriert sind, können Sie ein Ereignisabonnement erstellen, um festzulegen, welche Ereignisse weitergeleitet werden.

Mit quellinitiierten Abonnements (auch als *quellcomputerinitiierte Abonnements* bezeichnet) können Sie ein Abonnement auf einem Sammelcomputer konfigurieren, ohne die Quellcomputer anzugeben. Anschließend richten Sie über Gruppenrichtlinien mehrere Remotequellcomputer ein, sodass sie Ereignisse an den Sammelcomputer weiterleiten. Beim sammlungs-

initiierten Abonnementmodell müssen Sie dagegen alle Ereignisquellen direkt im Ereignisabonnement definieren.

Um den Sammelcomputer in einem quellinitiierten Abonnement zu konfigurieren, müssen Sie die Befehle in einer Eingabeaufforderung mit erhöhten Rechten eingeben. Befinden sich Sammel- und Quellcomputer in derselben Domäne, müssen Sie auf dem Sammelcomputer eine Ereignisabonnement-XML-Datei (beispielsweise unter dem Namen *Subscription.xml*) erstellen, eine Eingabeaufforderung mit erhöhten Rechten auf diesem Computer öffnen und die Windows-Remoteverwaltung konfigurieren, indem Sie den folgenden Befehl eingeben:

```
winrm qc -q
```

Dann konfigurieren Sie den Ereignissammlungsdienst auf demselben Computer, indem Sie den folgenden Befehl eingeben:

```
wecutil qc -q
```

Erstellen Sie ein quellinitiierte Abonnement auf dem Sammelcomputer, indem Sie diesen Befehl eingeben:

```
wecutil cs configuration.xml
```

Jedes Mal, wenn Sie einen Quellcomputer so konfigurieren, dass er ein quellinitiiertes Abonnement verwendet, müssen Sie auf diesem Computer zuerst die Windows-Remoteverwaltung konfigurieren, indem Sie den folgenden Befehl eingeben:

```
winrm qc -q
```

Anschließend verwenden Sie Gruppenrichtlinien, um die Adresse des Sammelcomputers zur Einstellung *SubscriptionManager* hinzuzufügen. Starten Sie zuerst den Gruppenrichtlinien-Editor, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten den folgenden Befehl eingeben:

```
%SystemRoot%\System32\gpedit.msc
```

Erweitern Sie im Editor für lokale Gruppenrichtlinien unter *Computerkonfiguration* die Zweige *Administrative Vorlagen* und *Windows-Komponenten*, und wählen Sie dann *Ereignisweiterleitung* aus. Beachten Sie, dass diese Option nicht zur Verfügung steht, wenn Sie Ihren Computer als Sammelcomputer konfiguriert haben.

Klicken Sie mit der rechten Maustaste auf die Einstellung *Serveradresse, Aktualisierungsintervall und Ausstellerzertifizierungsstelle eines Abonnement-Managers konfigurieren* (Kurzbezeichnung *SubscriptionManager*) und wählen Sie den Befehl *Eigenschaften*. Aktivieren Sie die Einstellung *SubscriptionManager* und klicken Sie auf die Schaltfläche *Anzeigen*. Fügen Sie mindestens eine Einstellung hinzu, die einen Sammelcomputer angibt. Das Eigenschaftenfenster der Einstellung *SubscriptionManager* enthält die Registerkarte *Erklärung*, auf der die Syntax der Einstellung beschrieben ist.

Führen Sie, nachdem Sie die Einstellung *SubscriptionManager* hinzugefügt haben, den folgenden Befehl aus, um sicherzustellen, dass die Richtlinie angewendet wird:

```
gpupdate /force
```

Erstellen eines Ereignisabonnements

Damit ein Sammelcomputer die Ereignisse empfängt, die von einem Quellcomputer übertragen werden, müssen Sie Ereignisabonnements erstellen. Bevor Sie ein Abonnement einrichten, müssen Sie die Sammlungs- und Quellcomputer wie oben beschrieben konfigurieren.

Gehen Sie folgendermaßen vor, um auf einem Sammelcomputer ein Abonnement zu erstellen:

1. Klicken Sie in der Ereignisanzeige mit der rechten Maustaste auf *Abonnements* und wählen Sie den Befehl *Abonnement erstellen*.
2. Klicken Sie auf *Ja*, falls Sie gefragt werden, ob der Windows-Ereignissammlungsdienst automatisch gestartet werden soll.
3. Geben Sie im Dialogfeld *Abonnementeigenschaften* (Abbildung 13.22) einen Namen für das Abonnement ein. Optional können Sie auch eine Beschreibung eingeben.

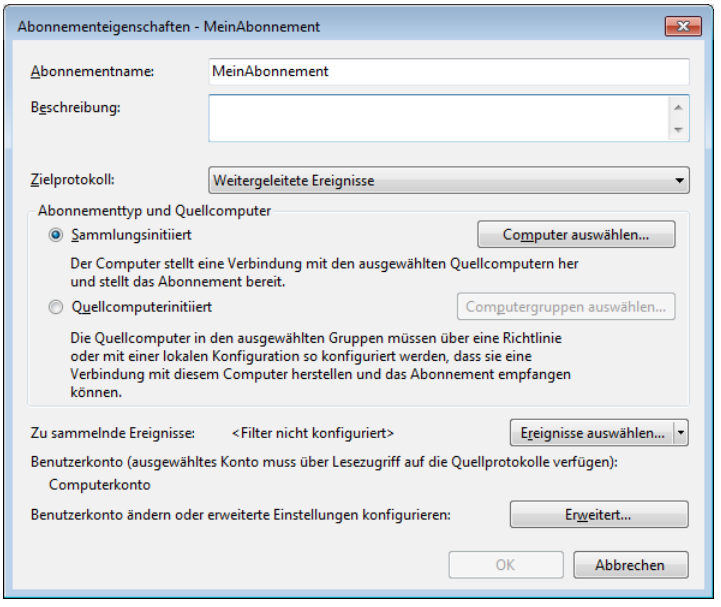

Abonnementeigenschaften - MeinAbonnement
Abonnementname:
MeinAbonnement
Beschreibung:
Zielprotokoll:
Weitergeleitete Ereignisse
Abonnementtyp und Quellcomputer
Sammlungsinitiiert
Computer auswählen...
Der Computer stellt eine Verbindung mit den ausgewählten Quellcomputern her und stellt das Abonnement bereit.
Quellcomputerinitiiert
Computergruppen auswählen...
Die Quellcomputer in den ausgewählten Gruppen müssen über eine Richtlinie oder mit einer lokalen Konfiguration so konfiguriert werden, dass sie eine Verbindung mit diesem Computer herstellen und das Abonnement empfangen können.
Zu sammelnde Ereignisse:
<Filter nicht konfiguriert>
Ereignisse auswählen...
Benutzerkonto (ausgewähltes Konto muss über Lesezugriff auf die Quellprotokolle verfügen):
Computerkonto
Benutzerkonto ändern oder erweiterte Einstellungen konfigurieren:
Erweitert...
OK
Abbrechen

Abbildung 13.22 Das Dialogfeld *Abonnementeigenschaften*

4. Wählen Sie den Abonnementtyp aus, den Sie erstellen wollen: *Sammlungsinitiiert* oder *Quellcomputerinitiiert*. Konfigurieren Sie den ausgewählten Abonnementtyp und geben Sie die Computer oder Computergruppen an.
5. Klicken Sie im Dialogfeld *Abonnementeigenschaften* auf die Schaltfläche *Ereignisse auswählen*, um das Dialogfeld *Abfragefilter* zu öffnen. Definieren Sie in diesem Dialogfeld, welche Kriterien weitergeleitete Ereignisse erfüllen müssen. Klicken Sie anschließend auf *OK*.
6. Wenn Sie wollen, können Sie im Dialogfeld *Abonnementeigenschaften* auf die Schaltfläche *Erweitert* klicken, um das Dialogfeld *Erweiterte Abonnementeinstellungen* zu öffnen. Sie können drei Arten von Abonnements konfigurieren: *Normal*, *Bandbreite minimieren* und *Wartezeit minimieren*.



Hinweis Auswählen des Kontos, das vom Abonnement benutzt wird

Im Dialogfeld *Erweiterte Abonnementeinstellungen* konfigurieren Sie auch, welches Konto das Abonnement benutzt. Unabhängig davon, ob Sie das Standardcomputerkonto oder ein Benutzerkonto verwenden, müssen Sie sicherstellen, dass dieses Konto auf dem Quellcomputer Mitglied der Gruppe *Ereignisprotokollleser* ist (oder, falls Sie Daten aus dem Sicherheitsereignisprotokoll überwachen, der lokalen Gruppe *Administratoren*).

7. Klicken Sie im Dialogfeld *Abonnementeigenschaften* auf *OK*, um das Abonnement zu erstellen.

Übung Ermitteln der aktuellen Datenträgerleistung mit der Leistungsüberwachung

In dieser Übung ermitteln Sie die aktuellen Leistungsdaten auf Ihrem Computer *Canberra*. Dann sehen Sie sich diese Daten im Kurven-, Histogramm- und Berichtsformat an. Der Computer in Ihrem Testnetzwerk liefert sicherlich andere Ergebnisse als der in diesem Beispiel. Bevor Sie diese Übung beginnen, müssen Sie ein zweites Speichergerät an den Computer anschließen, etwa eine zweite Festplatte oder einen USB-Flashstick.

Übung 1 Hinzufügen und Überwachen von Datenträgerleistungsindikatoren

In dieser Übung fügen Sie Leistungsindikatoren hinzu, mit denen Sie die Leistung des Systemvolumes (*C:*) überwachen. Falls Sie weitere Volumes auf derselben Festplatte oder mehrere Festplatten in Ihrem System haben, können Sie die Übung so erweitern, dass Sie auch diese Datenträger überwachen.



Hinweis *Diskperf*

In Windows 7 sind Leistungsindikatoren standardmäßig sowohl für logische als auch physische Datenträger aktiviert. Den Befehl `diskperf` gibt es weiterhin. Sie können damit für ältere Anwendungen, die mithilfe von `ioctl_disk_performance` ungefilterte Leistungsdaten abrufen, die Datenträgerleistungsindikatoren aktivieren oder deaktivieren.



Weitere Informationen Die Datei *Ioctl_disk_performance*

Weitere Informationen über *Ioctl_disk_performance* finden Sie unter *http://msdn.microsoft.com/en-us/library/ms804569.aspx*. Beachten Sie aber, dass dies ein älteres Feature ist, das in Prüfung 70-680 kaum behandelt werden dürfte.

Ein Engpass bei der Datenträgerlast und -geschwindigkeit hat deutliche Auswirkungen auf die Gesamtleistung eines Computers. Gehen Sie folgendermaßen vor, um Leistungsindikatoren hinzuzufügen, mit denen Sie die Datenträgerleistung überwachen:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Öffnen Sie die Leistungsüberwachung.
3. Klicken Sie in der Leistungsüberwachung auf die Schaltfläche *Hinzufügen* (mit dem grünen Plussymbol).

4. Stellen Sie im Dialogfeld *Leistungsindikatoren hinzufügen* sicher, dass in der Dropdownliste *Leistungsindikatoren auswählen von Computer* der Eintrag *<Lokaler Computer>* ausgewählt ist.
5. Aktivieren Sie das Kontrollkästchen *Beschreibung anzeigen*.
6. Wählen Sie alle Leistungsindikatoren aus, die momentan im Fensterabschnitt *Hinzugefügte Leistungsindikatoren* aufgelistet sind, und klicken Sie auf *Entfernen*.
7. Erweitern Sie in der Liste der verfügbaren Leistungsindikatoren den Eintrag *Logischer Datenträger* und wählen Sie *Freier Speicherplatz (%)* aus. Wählen Sie im Abschnitt *Instanzen des ausgewählten Objekts* den Eintrag *C:* aus (Abbildung 13.23). Der Leistungsindikator *Logischer Datenträger\Freier Speicherplatz (%)* misst, wie viel Prozent der Kapazität auf dem ausgewählten logischen Laufwerk frei sind. Wenn dieser Wert unter 15 Prozent fällt, besteht die Gefahr, dass dem Betriebssystem der Platz zum Speichern wichtiger Dateien ausgeht.

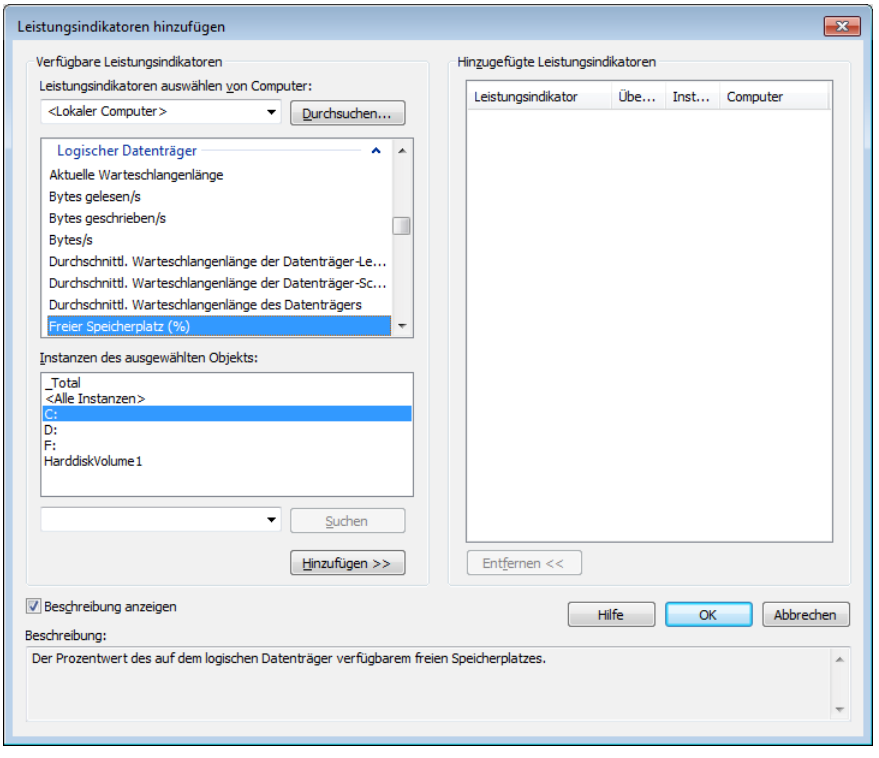


Abbildung 13.23 Auswählen der Instanz für den Leistungsindikator *Logischer Datenträger\Freier Speicherplatz (%)*

8. Klicken Sie auf *Hinzufügen*, um diesen Leistungsindikator hinzuzufügen.
9. Erweitern Sie in der Liste der verfügbaren Leistungsindikatoren den Eintrag *Physikalischer Datenträger* und wählen Sie *Leerlaufzeit (%)* aus. Wählen Sie im Abschnitt *Instanzen des ausgewählten Objekts* den Eintrag *C:* aus (Abbildung 13.24). Dieser Leistungsindikator misst, wie lange der Datenträger während des Messzeitraums im Leerlauf war. Fällt dieser Wert unter 20 Prozent, ist das Datenträgersystem stark ausge-

lastet; unter Umständen ist es dann angebracht, ein schnelleres Datenträgersystem zu installieren.

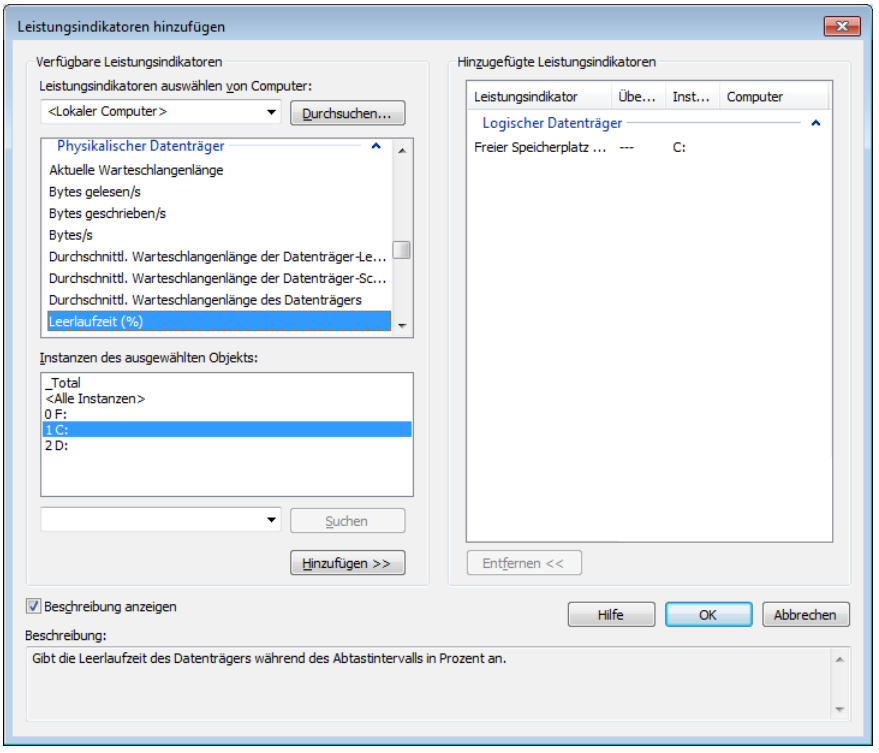


Abbildung 13.24 Auswählen des Leistungsindikators *Physikalischer Datenträger\ Leerlaufzeit (%)* für das Laufwerk *C:*

10. Klicken Sie auf *Hinzufügen*, um diesen Leistungsindikator hinzuzufügen.
11. Gehen Sie genauso vor, um die Instanz *C:* des Leistungsindikators *Physikalischer Datenträger\Mittlere Sek./Lesevorgänge* hinzuzufügen. Dieser Leistungsindikator misst, wie lange es durchschnittlich dauert, Daten vom Datenträger zu lesen. Ist dieser Wert größer als 25 ms (Millisekunden), tritt bei Leseoperationen vom Datenträger Latenz (Verzögerung) auf. In diesem Fall ist es möglicherweise sinnvoll, ein schnelleres Festplattensystem zu installieren.
12. Gehen Sie genauso vor, um die Instanz *C:* des Leistungsindikators *Physikalischer Datenträger\Mittlere Sek./Schreibvorgänge* hinzuzufügen. Dieser Leistungsindikator misst, wie lange es durchschnittlich dauert, Daten auf den Datenträger zu schreiben. Ist dieser Wert größer als 25 ms (Millisekunden), tritt bei Schreiboperationen auf dem Datenträger Latenz (Verzögerung) auf. In diesem Fall ist es möglicherweise sinnvoll, ein schnelleres Festplattensystem zu installieren.



Weitere Informationen **Der Leistungsindikator *Physikalischer Datenträger\Zeit (%)***

Weil der Wert im Leistungsindikator *Physikalischer Datenträger\Zeit (%)* 100 Prozent überschreiten kann, verwenden viele Administratoren lieber die Leistungsindikatoren *Physikalischer Datenträger\Leerlaufzeit (%)*, *Physikalischer Datenträger\Mittlere Sek./Lesevorgänge* und *Physikalischer Datenträger\Mittlere Sek./Schreibvorgänge*, um sich ein genaueres Bild von der Festplattenauslastung zu machen. Weitere Informationen über den Leistungsindikator *Physikalischer Datenträger\Zeit (%)* finden Sie unter *http://support.microsoft.com/kb/310067*.

13. Gehen Sie genauso vor, um die Instanz *C:* des Leistungsindikators *Physikalischer Datenträger\Durchschnittl. Warteschlangenlänge des Datenträgers* hinzuzufügen. Dieser Leistungsindikator gibt an, wie viele E/A-Operationen darauf warten, dass der Datenträger verfügbar wird. Ist der Wert dieses Leistungsindikators größer als das Doppelte der Zahl von Einzelfestplatten in einem Laufwerkarray, bildet möglicherweise die Festplatte den Engpass.
14. Gehen Sie genauso vor, um den Leistungsindikator *Arbeitsspeicher\Cachebytes* hinzuzufügen. Dieser Leistungsindikator gibt an, wie viel Arbeitsspeicher für den Dateisystemcache benutzt wird. Ein möglicher Datenträgerengpass liegt vor, wenn dieser Wert über 300 MByte steigt.
15. Prüfen Sie, ob das Dialogfeld *Leistungsindikatoren hinzufügen* dieselben Leistungsindikatoren und Instanzen wie Abbildung 13.25 enthält. Klicken Sie auf *OK*.

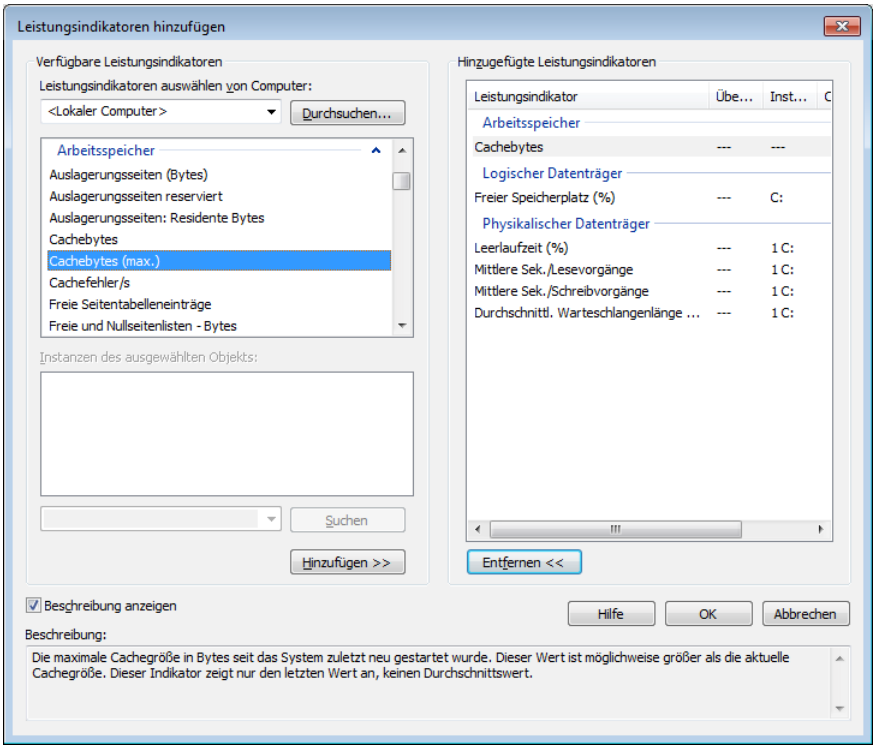


Abbildung 13.25 Die benötigten Leistungsindikatoren und Instanzen wurden ausgewählt



Hinweis Standardmäßig verwendete Leistungsindikatoren

Der Leistungsindikator *Prozessor\Prozessorzeit (%)* ist standardmäßig enthalten, daher brauchen Sie ihn nicht hinzuzufügen. Er taucht in der Liste in Abbildung 13.25 nicht auf, aber Sie sehen ihn in den Linien-, Histogramm- und Berichtansichten in Übung 2.

16. Schließen Sie die Leistungsüberwachung noch nicht. Fahren Sie direkt mit Übung 2 fort.

Übung 2 Konfigurieren der Leistungsüberwachung und Überwachen der Datenträgerleistung

In dieser Übung stellen Sie Frequenz und Gesamtdauer der Messung ein, lesen und schreiben Daten auf dem Datenträgervolume, das Sie überwachen, und sehen sich die Ergebnisse im Kurven-, Histogramm- und Berichtsformat an. Führen Sie diese Übung unmittelbar nach Übung 1 durch.

1. Klicken Sie im Fensterabschnitt *Aktionen* der Leistungsüberwachung auf *Weitere Aktionen* und wählen Sie den Befehl *Eigenschaften*.
2. Ändern Sie auf der Registerkarte *Allgemein* des Dialogfelds *Eigenschaften von Leistungsüberwachung* im Abschnitt *Diagrammelemente* den Wert unter *Stichprobe alle* auf 5 und den Wert *Dauer* auf 300. Klicken Sie auf *OK*.
3. Kopieren Sie eine Datei oder einen Ordner (sie sollten größer als 100 MByte sein) von Ihrem Laufwerk *C:* auf das zweite angeschlossene Speichergerät.
4. Kopieren Sie eine Datei oder einen Ordner (größer als 100 MByte) von Ihrem zweiten angeschlossenen Speichergerät auf Laufwerk *C:*.

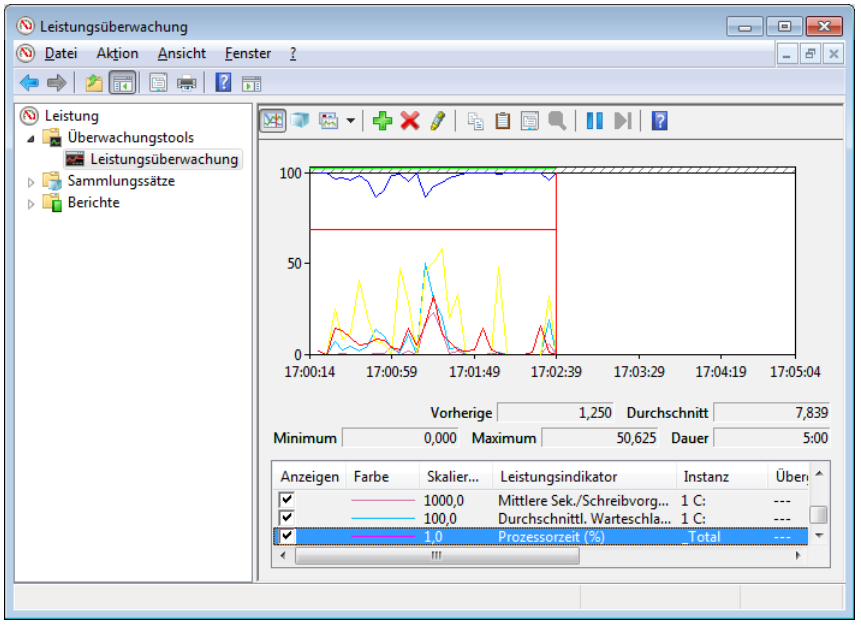


Abbildung 13.26 Kurvendiagramm in der Leistungsüberwachung

5. Sehen Sie sich in der Leistungsüberwachung das Kurvendiagramm genau an (Abbildung 13.26). Oft ist es schwierig, hier die Informationen zu finden, die Sie tatsächlich brauchen.

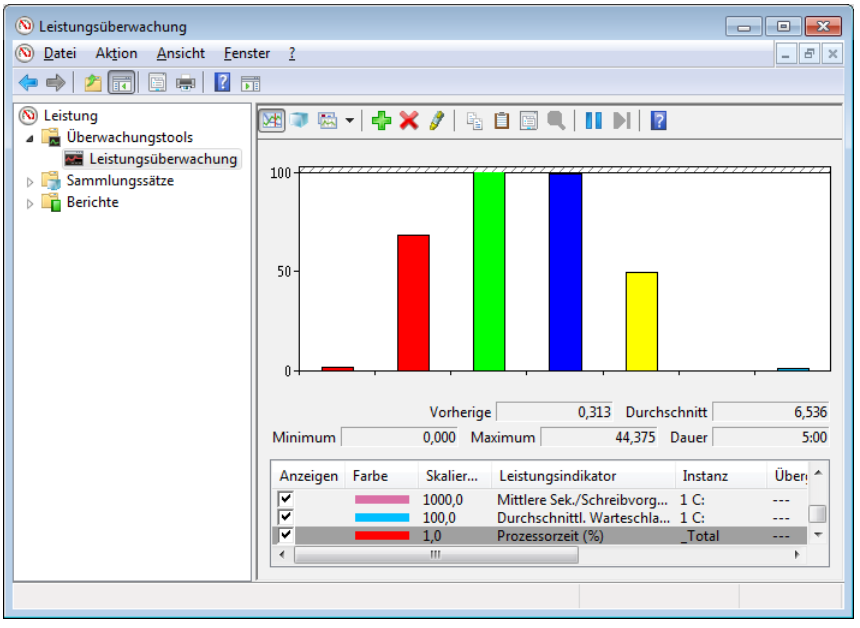


Abbildung 13.27 Histogrammansicht in der Leistungsüberwachung

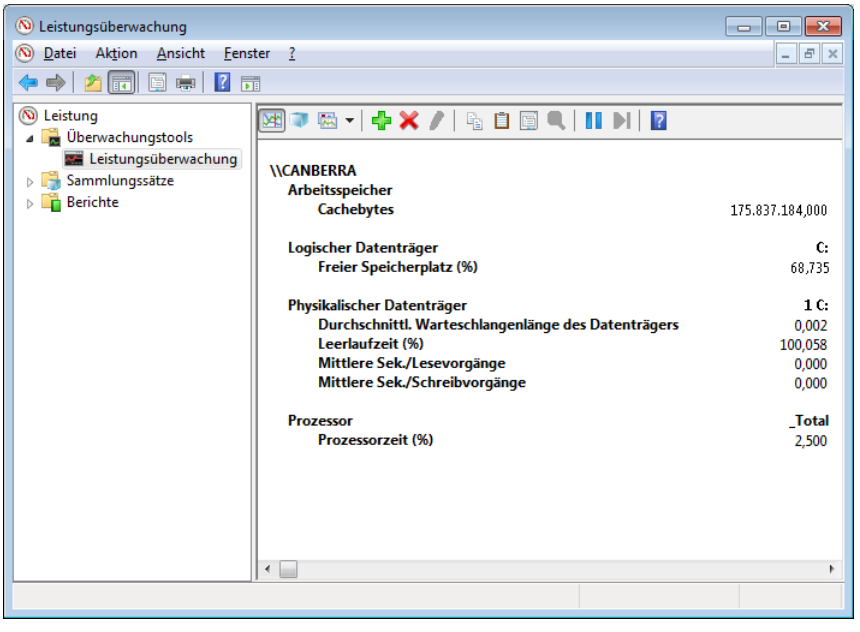


Abbildung 13.28 Berichtansicht in der Leistungsüberwachung

6. Wählen Sie in der Dropdownliste *Diagrammtyp ändern* den Eintrag *Histogrammleiste* aus. Sehen Sie sich das Histogramm in der Leistungsüberwachung genau an (Abbildung 13.27).
7. Wählen Sie in der Dropdownliste *Diagrammtyp ändern* den Eintrag *Bericht* aus. Sehen Sie sich den Bericht in der Leistungsüberwachung an (Abbildung 13.28).
8. Analysieren Sie die Leistungsindikatorwerte unter Berücksichtigung dessen, was Sie in Übung 1 über die verschiedenen Leistungsindikatoren gelernt haben. Die Ergebnisse in den Abbildungen zeigen, dass auf Volume *C:* genug Platz frei ist und beim Kopieren relativ großer Dateien oder Ordner kein Problem auftrat. Die Cachespeichernutzung war erheblich, aber das ist bei diesem Vorgang normal und kein Grund zur Besorgnis. Auf Ihrem Testrechner erhalten Sie selbstverständlich andere Ergebnisse.



Hinweis Dateicache

Damit Sie aussagekräftige Ergebnisse bekommen, werden Sie in Übung 2 aufgefordert, sich Kurven-, Histogramm- und Berichtansichten für dieselben Kopieroperationen anzusehen. Würden Sie die Kopieroperationen wiederholen, um sich jeweils die Histogramm- und Berichtansichten anzusehen, bekämen Sie unterschiedliche Ergebnisse. Windows 7 schreibt die Datei oder den Ordner beim Kopieren nämlich in einen Cache. Die Ergebnisse der nachfolgenden Operationen würden dann nur wiedergeben, wie die Datei aus dem RAM ausgelesen und auf Festplatte geschrieben wird. Die Tools zu verwenden, ist oft ganz simpel. Die Ergebnisse richtig zu interpretieren, ist nicht immer so einfach.

Zusammenfassung der Lektion

- Sie können sich in der Leistungsüberwachung Leistungsdaten in Echtzeit ansehen oder Leistungsindikatorwerte, die Sie in Sammlungssätzen aufgezeichnet haben. Ein Systemdiagnosebericht liefert Details über den Status von Hardwareressourcen, Systemreaktionszeiten und Prozesse auf dem lokalen Computer sowie Systeminformationen und Konfigurationsdaten.
- Die Zuverlässigkeitsüberwachung verfolgt die Stabilität eines Computers. Sie verrät Ihnen auch, wann Ereignisse aufgetreten sind, die sich auf die Stabilität auswirken (beispielsweise die Installation einer Softwareanwendung), und ob nach diesen Ereignissen Neustarts notwendig waren. Das Wartungscenter überwacht Ihren Computer und meldet Probleme in den Bereichen Sicherheit, Wartung und den zugehörigen Einstellungen. Der Windows-Leistungsindex gibt einen Anhaltspunkt, wie gut sich Ihre aktuelle Computerhardware für ressourcenintensive Anwendungen eignet.
- Der Task-Manager liefert eine Momentaufnahme der Ressourcenauslastung. Außerdem können Sie darin Anwendungen, Dienste und Protokolle verwalten. Im Ressourcenmonitor bekommen Sie in Echtzeit Informationen über die Auslastung von Hardware- und Softwareressourcen angezeigt. Der Process Explorer erfüllt eine ähnliche Funktion wie der Task-Manager, bietet aber mehr Eingriffsmöglichkeiten und liefert detailliertere Systeminformationen.

- In der Ereignisanzeige können Sie Ereignisprotokolle auswerten und filtern. Dabei haben Sie die Möglichkeit, benutzerdefinierte Ansichten zu erstellen. Sie können Aufgaben mit Ereignissen verknüpfen und Ereignisweiterleitung und Ereignisabonnements konfigurieren, damit ein zentraler Computer Ereignisse speichert, die auf einem oder mehreren Quellcomputern generiert werden.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Überwachen von Systemen«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie haben die Hardware eines Computers aufgerüstet, damit er sich für eine Anwendung eignet, die den Prozessor stark belastet. Sie lassen vom Tool Windows-Leistungsindex eine neue Gesamtbewertung erstellen. Die Teilnoten für jede Komponente sind:
   - Prozessor 5,1
   - Arbeitsspeicher (RAM) 3,3
   - Grafik 3,6
   - Grafik (Spiele) 2,3
   - Primäre Festplatte 5,3

   Welchen Wert hat der Windows-Leistungsindex?
   A. 2,3
   B. 3,9
   C. 5,1
   D. 4,4
2. Bei einem Windows 7-Client treten sporadisch Leistungsprobleme auf. Sie vermuten, dass die Probleme durch eine Anwendung verursacht werden, die Sie vor Kurzem installiert haben. Sie haben aber vergessen, wann genau Sie die Installation durchgeführt haben. Mit welchem Tool oder Feature stellen Sie fest, wann die Anwendung installiert wurde?
   A. Zuverlässigkeitsüberwachung
   B. Wartungscenter
   C. Sammlungssätze
   D. Leistungsüberwachung
3. Welche der folgenden Informationen werden in der Zuverlässigkeitsüberwachung gespeichert? (Wählen Sie alle zutreffenden Antworten aus; sie bilden zusammen die vollständige Lösung.)

A. Eine Anwendung stürzt ab und muss neu gestartet werden.
B. Ein Windows-Fehler tritt auf und das System muss neu gestartet werden.
C. Eine Anwendung wird deinstalliert.
D. Ein Dienst wird beendet.
E. Ein Gerätetreiber stürzt ab.

4. Sie konfigurieren einen Windows 7-Client namens *Canberra*, um Ereignisse vom Windows 7-Computer *Aberdeen* abzurufen. Beide Computer sind Mitglieder derselben Arbeitsgruppe. Welchen der folgenden Befehle führen Sie auf dem Sammelcomputer aus, um den Ereignissammlungsdienst zu konfigurieren?
   A. `wecutil qc`
   B. `winrm qc`
   C. `winrm qc -q`
   D. `%SystemRoot%\System32\gpedit.msc`
5. Sie wollen in der Leistungsüberwachung Leistungsdaten anzeigen, die Sie in einem Sammlungssatz aufgezeichnet haben. Sie starten das Tool und öffnen das Dialogfeld *Eigenschaften von Leistungsüberwachung*. Auf welcher Registerkarte wählen Sie aus, ob die aktuelle Aktivität in Echtzeit oder die Protokolldateien angezeigt werden, die Sie mit einem Sammlungssatz gespeichert haben?
   A. *Allgemein*
   B. *Quelle*
   C. *Daten*
   D. *Grafik*
   E. *Darstellung*

Lektion 2: Konfigurieren von Leistungseinstellungen

Diese Lektion beschreibt, welche Einstellungen die Leistung Ihres Computers beeinflussen und welche Tools Windows 7 zur Verfügung stellt, um Leistungseinstellungen anzuzeigen und zu ändern und um Leistungsprobleme zu beseitigen. Wenn Sie die integrierten Tools nicht mögen, können Sie mithilfe von WMI-Skripts (Windows Management Instrumentation) eigene schreiben.

Viele Faktoren haben Auswirkung auf die Leistung, etwa die Darstellung Ihres Bildschirms oder Ihres Browserfensters, die Dienste und Prozesse, die auf dem Computer laufen, und die Priorität und Prozessorzugehörigkeit, die Sie verschiedenen Prozessen zuordnen. Die Leistung wird durch Ihre Einstellungen für Cache und Auslagerungsdateien beeinflusst, durch die Dienste und Anwendungen, die automatisch starten oder laufen, obwohl sie nicht benötigt werden, und dadurch, welche Prozesse ausgeführt werden und welche Ressourcen sie verbrauchen.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Benutzen verschiedener Windows-Tools, um Einstellungen zu prüfen und zu konfigurieren, die sich auf die Windows 7-Leistung auswirken
- Schreiben von WMI-Skripts, die Systeminformationen zurückliefern, und Benutzen der WMI-Tools.
- Beseitigen von Leistungsproblemen

Veranschlagte Zeit für diese Lektion: 45 Minuten

Abrufen von Systeminformationen mit WMI

Mit WMI können Sie auf Systemverwaltungsinformationen zugreifen. Es wurde so entworfen, dass es über ein Netzwerk hinweg arbeitet. Es stellt ein konsistentes Modell der verwalteten Umgebung und für jede verwaltbare Ressource eine WMI-Klasse zur Verfügung. Eine WMI-Klasse ist eine Beschreibung der Eigenschaften einer verwalteten Ressource sowie der Aktionen, die WMI ausführen kann, um diese Ressource zu verwalten. Eine verwaltete Ressource ist irgendein Objekt (Computerhardware, Computersoftware, Dienst oder Benutzerkonto), das mithilfe von WMI verwaltet werden kann.

Sie setzen WMI ein, indem Sie Skripts schreiben, die auf die WMI-Skriptingbibliothek zurückgreifen. Diese Bibliothek ermöglicht Ihnen, mit WMI-Klassen zu arbeiten, die verwaltete Ressourcen abbilden. Mithilfe dieses Ansatzes können Sie Ressourcen wie Festplattenlaufwerke, Ereignisprotokolle und installierte Software verwalten.

Sie können Windows Script Host (WSH), Microsoft Visual Basic Scripting Edition (VBScript), Microsoft JScript oder Skriptsprachen wie ActivePerl verwenden, um WMI-Skripts zu schreiben, die Verwaltungsaufgaben in Ihrem Netzwerk automatisieren. Üblicherweise haben WMI-Skriptdateien die Erweiterung *.vbs*.

Sie können Skripts schreiben, um Ereignisprotokolle, Dateisysteme, Drucker, Prozesse, Registrierungseinstellungen, geplante Aufgaben, Sicherheit, Dienste, freigegebene Ordner und vieles andere zu verwalten. Sie können WMI-Skripts schreiben, die Netzwerkdienste wie DNS (Domain Name System) und clientseitige Netzwerkeinstellungen verwalten. So stellen Sie zum Beispiel ein, ob ein Computer mit statischen IPv4-Adresseinstellungen (Internet Protocol Version 4) konfiguriert wird oder diese Einstellungen von einem DHCP-

Server (Dynamic Host Configuration Protocol) abruft. WMI-Skripts können Einträge in einem Ereignisprotokoll, Veränderungen am Dateisystem oder der Registrierung und andere Echtzeitveränderungen im Betriebssystem überwachen und darauf reagieren.

Ein WMI-Skript arbeitet mit WMI-Klassen, die physische Komponenten oder Dienste auf einem Computer abbilden. Jede Klasse kann Objekte oder Instanzen enthalten, und die Objekte haben Attribute. Sie können den Wert jedes Attributs anzeigen oder ihn zu Analysezwecken an eine andere Routine übergeben.

Normalerweise schreiben Sie WMI-Skripts in einem Texteditor wie dem Windows-Editor und speichern sie als *.vbs*-Dateien in einem Verzeichnis (zum Beispiel *C:\WMI_Scripts*), das Sie für diesen Zweck angelegt haben. Passen Sie auf, wenn Sie Textverarbeitungssoftware wie Microsoft Office Word für diese Aufgabe einsetzen. Textverarbeitungssoftware verwendet in unterschiedlichen Schriftarten oft andere Anführungszeichen (nur ein Beispiel), was unter Umständen Syntaxfehler auslöst. Sie können WMI-Skripts in einer Eingabeaufforderung mit erhöhten Rechten ausführen, indem Sie das Programm Cscript verwenden. Sie können auch Batchdateien erstellen, die Skripts in regelmäßigen Abständen ausführen oder durch ein Ereignis gestartet werden.

Das folgende WMI-Skript greift auf Instanzen der Klasse `Win32_Battery` zu (es gibt davon allerdings nur eine Instanz) und gibt den Wert des Attributs `EstimatedChargeRemaining` aus. Der Code sieht komplexer aus, als er in Wirklichkeit ist.

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\" & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf("Win32_Battery")
For Each objSWbemObject In colSWbemObjectSet
  Wscript.Echo "Verbleibende Kapazität: " & objSWbemObject.EstimatedChargeRemaining &
  " Prozent."
Next
```

Abbildung 13.29 zeigt die Ausgabe dieser Skriptdatei, die unter dem Namen *Battery.vbs* im Ordner *C:\WMI_Skripts* gespeichert wurde. Wenn Sie dieses Skript auf einem Desktopcomputer ausführen, müsste es ohne Fehler durchlaufen, aber nichts ausgeben.

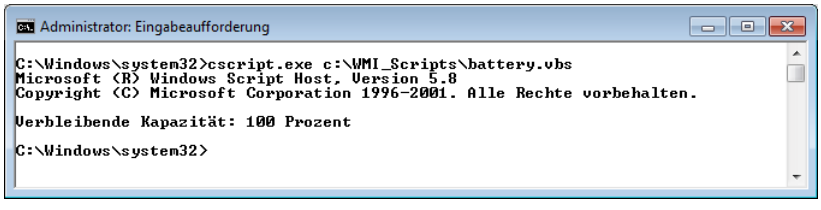

Administrator: Eingabeaufforderung
C:\Windows\system32>cscript.exe c:\WMI_Scripts\battery.vbs
Microsoft (R) Windows Script Host, Version 5.8
Copyright (C) Microsoft Corporation 1996-2001. Alle Rechte vorbehalten.
Verbleibende Kapazität: 100 Prozent
C:\Windows\system32>

Abbildung 13.29 Ein WMI-Skript liest die verbleibende Akkukapazität aus

Sie können andere WMI-Klassen verwenden und die Werte ihrer Attribute herausfinden, indem Sie den Namen der Klasse und der Attribute in diesem Skript austauschen. Zum Beispiel ist `FreePhysicalMemory` ein Attribut der Objekte in der Klasse `Win32_OperatingSystem` (normalerweise gibt es in dieser Klasse nur ein Objekt). Das folgende WMI-Skript gibt aus, wie viel physischer Arbeitsspeicher (in der Einheit KByte) auf einem Computer frei ist:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\" & strComputer)
```

```
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_OperatingSystem")
For Each objSWbemObject In colSWbemObjectSet
  Wscript.Echo "Freier physischer Speicher: " & objSWbemObject.FreePhysicalMemory & " KB."
Next
```

Abbildung 13.30 zeigt die Ausgabe dieser Skriptdatei, nachdem sie unter *Memory.vbs* im Ordner *C:\WMI_Skripts* gespeichert wurde.

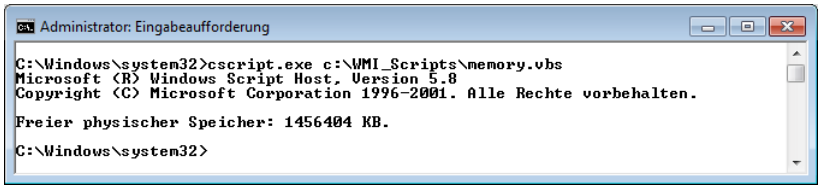

Administrator: Eingabeaufforderung
C:\Windows\system32>cscript.exe c:\WMI_Scripts\memory.vbs
Microsoft (R) Windows Script Host, Version 5.8
Copyright (C) Microsoft Corporation 1996-2001. Alle Rechte vorbehalten.
Freier physischer Speicher: 1456404 KB.
C:\Windows\system32>

Abbildung 13.30 Ein WMI-Skript ermittelt, wie viel physischer Arbeitsspeicher noch frei ist



Weitere Informationen **Liste der WMI-Klassen**

Eine Liste aller WMI-Klassen und ihrer Attribute finden Sie unter *http://msdn.microsoft.com/en-us/library/aa394554(VS.85).aspx*. Die vollständige WMI-Referenz enthält *http://msdn.microsoft.com/en-us/library/aa394572(VS.85).aspx*.



Warnung **WMI-Klassen**

Wenn Sie eine WMI-Klasse benutzen, müssen Sie sicherstellen, dass Windows 7 sie auch unterstützt. Beispielsweise wurde die Klasse `Win32_LogicalMemoryConfiguration` verworfen, sie wird daher nicht mehr unterstützt. Wenn Sie diese Klasse in einem Skript verwenden, das Sie auf einem Windows 7-Computer ausführen, wird der Fehler 0x80041010 ausgelöst.

Sie können in Skripts auch WMI-Klassen verwenden, die mehrere Objekte umfassen. So enthält die Klasse `Win32_Services` alle Dienste, die auf einem Computer laufen. Das folgende Skript listet all diese Dienste auf:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\" & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_Service")
For Each objSWbemObject In colSWbemObjectSet
  Wscript.Echo "Anzeigename: " & objSWbemObject.DisplayName & vbCrLf
Next
```

Wenn Sie das letzte Skript etwas ausbauen, können Sie auch den Status (gestartet oder beendet) und den Startmodus für jeden Dienst ermitteln:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\" & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_Service")
For Each objSWbemObject In colSWbemObjectSet
  Wscript.Echo "Anzeigename: " & objSWbemObject.DisplayName & vbCrLf
    & " Status: " & objSWbemObject.State & vbCrLf
    & " Startmodus: " & objSWbemObject.StartMode
Next
```

Abbildung 13.31 zeigt einen Ausschnitt aus der Ausgabe dieses Skripts.

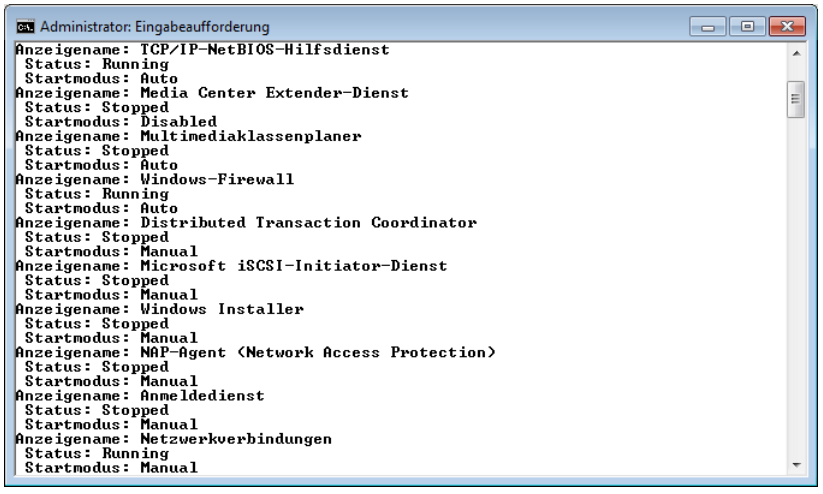


Abbildung 13.31 Ermitteln von Status und Startmodus aller Dienste

Sie setzen WMI ein, um verwaltete Ressourcen zu administrieren. Dazu gehören unter anderem das Computersystem, Active Directory-Domänendienste (Active Directory Domain Services, AD DS), Datenträger, Peripheriegeräte, Ereignisprotokolle, Dateien, Ordner, Dateisysteme, Netzwerkkomponenten, Subsysteme des Betriebssystems, Leistungsindikatoren, Drucker, Prozesse, Registrierungseinstellungen, Sicherheit, Dienste, freigegebene Ordner, Benutzer und Gruppen, Windows Installer, Gerätetreiber und SNMP-MIB-Daten (Simple Network Management Protocol-Management Information Base).

Wenn Sie Skripts schreiben, die auf WMI-verwaltete Ressourcen zugreifen, bezieht sich der Begriff *Instanz* auf eine verwaltete Ressource im Skript. Zum Beispiel gibt das folgende Skript den Laufwerkbuchstaben für jedes logische Festplattenlaufwerk auf Ihrem Computer zurück:

```
strComputer = "."
Set objSWbemServices = GetObject("winmgmts:\\" & strComputer)
Set colSWbemObjectSet = objSWbemServices.InstancesOf ("Win32_LogicalDisk")
For Each objSWbemObject In colSWbemObjectSet
  Wscript.Echo objSWbemObject.DeviceID
Next
```

Sie können in einem WMI-Skript eine Eingabe anfordern und den Text in einer Variablen speichern. Das folgende Skript (beziehungsweise ein Ausschnitt daraus) fordert den Benutzer auf, ein Kennwort einzugeben, und speichert es in der Stringvariablen `strPassword`. Diese Variable können Sie anschließend beispielsweise an die Funktion `Connect.Server` übergeben, um eine Verbindung zu einem Server im Netzwerk herzustellen:

```
strComputer = "."
Wscript.StdOut.Write "Geben Sie bitte das Administratorkennwort ein: "
strPassword = Wscript.StdIn.ReadLine
```

Das nächste Skript ist eine vollständige Routine, die Sie für Ihre eigenen Zwecke übernehmen können. Es ruft die Funktion `inputbox` auf, um die Eingabe eines Computernamens an-

zufordern, und zeigt dann mit der Funktion `MsgBox` Informationen über Drucker, Prozesse und CPU dieses Computers an. Der Code ist nicht wesentlich komplexer als in den letzten Beispielen (er zeigt einfach die Werte von Objektattributen an), aber die Aufrufe der eingebauten Funktionen geben dem Skript einen professionellen Anstrich:

```
computer = inputbox ("Welchen Computer möchten Sie untersuchen? (Eingabetaste für diesen
Computer)","Computer")
set WMI = GetObject("WinMgmts://" & computer)
If computer="" then computer = "diesem Computer"
List = ""
Set objs = WMI.InstancesOf("Win32_Printer")
For each obj in objs
  List = List & obj.Caption & ", "
Next
List=Left(List, Len(List)-2)
MsgBox List,64,"Drucker an " & computer
List = ""
Set objs = WMI.InstancesOf("Win32_Process")
For each obj in objs
  List = List & obj.Description & ", "
Next
List=Left(List, Len(List)-2)
MsgBox List,64,"Prozesse in " & computer
List = ""
set objs = WMI.InstancesOf("Win32_Processor")
For each obj in objs
  List = List & obj.Description & ", "
Next
List=Left(List, Len(List)-2)
MsgBox List,64,"CPU in " & computer
```

Wenn Sie den Computer *Aberdeen* angeben, während Sie das Skript auf *Canberra* ausführen, müssen Sie sicherstellen, dass das Konto *\\Canberra\Kim_Akers* Administratorprivilegien auf *Aberdeen* hat. Nur ein lokaler Administrator kann ein WMI-Skript auf einem Computer ausführen. Wenn Sie allerdings die erforderlichen Rechte haben, ist es ganz einfach, WMI-Skripts auf Remotecomputern auszuführen. Das Skript ist wahrscheinlich eher für Unternehmensumgebungen sinnvoll, wo die Gruppen *Domänen-Admins* und *Organisations-Admins* auf allen Computern entsprechende Berechtigungen haben. Stellen Sie auch sicher, dass keine Firewalls die Daten blockieren. Abbildung 13.32 zeigt, wie die Liste der Prozesse auf *Canberra* in einem Meldungsfeld angezeigt wird.

WMI besteht aus drei Hauptkomponenten: CIMOM (Common Information Model Object Manager), auch als WMI-Dienst bezeichnet; CIM-Repository (Common Information Model), auch als WMI-Repository bezeichnet; und WMI-Anbietern. Zusammen stellen diese Komponenten eine Infrastruktur zur Verfügung, über die Konfigurations- und Verwaltungsdaten definiert, zugänglich gemacht, verändert und abgerufen werden.

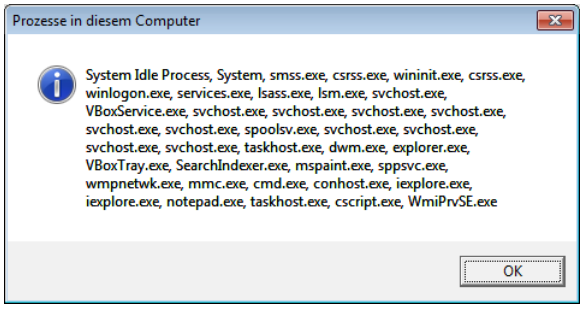

Prozesse in diesem Computer
System Idle Process, System, smss.exe, csrss.exe, wininit.exe, csrss.exe, winlogon.exe, services.exe, lsass.exe, lsm.exe, svchost.exe, VBoxService.exe, svchost.exe, svchost.exe, svchost.exe, svchost.exe, svchost.exe, svchost.exe, spoolsv.exe, svchost.exe, svchost.exe, svchost.exe, svchost.exe, taskhost.exe, dwm.exe, explorer.exe, VBoxTray.exe, SearchIndexer.exe, mspaint.exe, sppsvc.exe, wmpnetwk.exe, mmc.exe, cmd.exe, conhost.exe, iexplore.exe, iexplore.exe, notepad.exe, taskhost.exe, cscript.exe, WmiPrvSE.exe
OK

Abbildung 13.32 Prozesse auf diesem Computer (*Canberra*)

WMI-Anbieter

WMI-Anbieter (WMI provider), beispielsweise Win32 und der integrierte Ereignisprotokollanbieter, agieren als Vermittler zwischen dem CIMOM und einer verwalteten Ressource. Anbieter fordern im Auftrag von Anwendungen und Skripts Informationen von WMI-verwalteten Ressourcen an und senden ihnen Anweisungen. Anbieter machen die verwaltete Ressource in der WMI-Infrastruktur über ein standardkonformes Zugriffsmodell zugänglich, kommunizieren mit den zugehörigen verwalteten Ressourcen über die nativen Programmierschnittstellen (Application Programming Interface, API) der verwalteten Ressource und kommunizieren mit dem CIMOM über die WMI-Programmierschnittstellen. Windows 7 führt neue Anbieter für Windows PowerShell und Virtualisierung ein.

Wenn Sie eine Anwendung erstellen, die Windows-Subsysteme verwaltet, verwenden Sie meist die Win32-APIs. Ohne WMI müssten Sie diese APIs selbst aufrufen. Leider können Win32-APIs nicht aus einem Skript heraus aufgerufen werden, Sie müssten also eine Programmiersprache wie C++ oder Microsoft Visual Basic verwenden. Es ist viel schwieriger, C++- oder Visual Basic-Code zu schreiben als ein Skript.

Wenn Sie WMI-Anbieter benutzen, brauchen Sie sich nicht darum zu kümmern, wie die Win32-APIs aufgerufen werden, weil WMI das für Sie erledigt. Sie müssen sich auch nicht über die Unterschiede zwischen verschiedenen APIs den Kopf zerbrechen, weil Sie einen Standardsatz WMI-Befehle verwenden, die WMI in Befehle übersetzt, die von den APIs verstanden werden.

WMI-Anbieter sind im Allgemeinen als DLLs im Verzeichnis *SystemRoot\System32\Wbem* implementiert. Die integrierten Anbieter, auch als *Standardanbieter* (default provider) bezeichnet, stellen Daten- und Verwaltungsfunktionen von bekannten Betriebssystemquellen zur Verfügung, beispielsweise aus dem Win32-Subsystem, Ereignisprotokollen, Leistungsindikatoren und der Registrierung.

Der CIMOM

Der CIMOM erledigt die Interaktion zwischen Verbrauchern und Anbietern. Er agiert als WMI-Informationsbroker. Alle WMI-Anforderungen und -Daten fließen durch den CIMOM. Wenn Sie ein WMI-Skript schreiben, wird es an den CIMOM geleitet. Der CIMOM verarbeitet Ihre Anforderung allerdings nicht direkt. Nehmen wir an, Sie fordern eine Liste aller Dienste an, die auf einem Computer installiert sind. Der CIMOM ruft die Liste der Dienste nicht selbst für Sie ab. Stattdessen sucht er den passenden WMI-Anbieter und fordert ihn auf, die Liste zu liefern. Sobald die Liste vorliegt, gibt der CIMOM die Informationen an Sie zurück.

Der WMI-Dienst

Der WMI-Dienst (*Winmgmt.exe*) implementiert den CIMOM unter Windows 7. Sie können ihn in einer Eingabeaufforderung mit erhöhten Rechten starten und beenden, wie jeden anderen Dienst auch (beispielsweise mit `net stop winmgmt`). Passen Sie aber auf: Wenn Sie den WMI-Dienst beenden, laufen auch das Sicherheitscenter und IP-Hilfsdienste nicht mehr. Wurde der WMI-Dienst beendet, wenn Sie ein Skript oder eine Anwendung ausführen, die WMI benötigt, wird der Dienst automatisch neu gestartet.

Das CIM-Repository

Verwaltungsanwendungen, Verwaltungstools und Skripts senden Anforderungen an den CIMOM, um Daten abzurufen, Ereignisse zu abonnieren oder andere Verwaltungsaufgaben durchzuführen. Der CIMOM ermittelt aus dem CIM-Repository, welcher Anbieter und welche Klasseninformationen gebraucht werden, um die Verbraucheranforderungen zu bedienen. Anhand der Informationen, die der CIMOM aus dem CIM-Repository erhalten hat, leitet er die Verbraucheranforderungen an den passenden WMI-Anbieter weiter.

Das CIM-Repository speichert das Schema, auch als *Objektrepository* (object repository) oder *Klassenspeicher* (class store) bezeichnet, das alle Daten definiert, die über WMI zur Verfügung gestellt werden. Das Schema ähnelt dem AD DS-Schema, es ist auf dem Konzept von Klassen aufgebaut. Eine Klasse ist eine Art Bauplan für eine WMI-verwaltbare Ressource. Im Unterschied zu AD DS-Klassen repräsentieren die meisten CIM-Klassen allerdings dynamische Ressourcen. Instanzen von Ressourcen werden nicht im CIM-Repository gespeichert, sondern dynamisch von einem Anbieter abgerufen, sobald eine Verbraucheranforderung eintrifft. Das bedeutet, dass der Begriff *Repository* etwas irreführend ist. Das CIM ist zwar ein Repository, das in der Lage ist, statische Daten zu speichern, aber seine Hauptaufgabe besteht darin, die Baupläne für verwaltete Ressourcen zu speichern.

Der Status ändert sich bei den meisten WMI-verwalteten Ressourcen recht häufig (denken Sie nur an die vielen Ereignisse in allen Ereignisprotokollen eines Computers). Sie werden erst auf Anforderung ausgelesen, um sicherzustellen, dass die neuste Version der Daten abgerufen wird. Das kann gelegentlich dazu führen, dass Abfragen langsam laufen, wenn sehr viele Informationen abgerufen werden müssen, aber das ist immer noch besser, als die Ressourcen des Computers damit zu belasten, ein immer aktuelles Repository mit Daten zu pflegen, die sich ständig ändern.

CIM-Klassen

CIM-Klassen sind hierarchisch organisiert. Untergeordnete Klassen werden von übergeordneten Klassen abgeleitet. Die DMTF (Distributed Management Task Force) verwaltet einen Satz Kern- und wichtiger Basisklassen, von denen System- und Anwendungssoftwareentwickler system- oder anwendungsspezifische Erweiterungsklassen ableiten. Die Klassen werden in Namespaces zusammengefasst. Dies sind logische Gruppen, die einen bestimmten Verwaltungsbereich abgrenzen. CIM-Klassen haben sowohl Eigenschaften als auch Methoden. Eigenschaften beschreiben die Konfiguration und den Zustand einer WMI-verwalteten Ressource. Methoden sind ausführbare Funktionen, die Aktionen mit der WMI-verwalteten Ressource ausführen, die mit der entsprechenden Klasse verknüpft ist.



Weitere Informationen DMTF

Weitere Informationen über die Distributed Management Task Force finden Sie auf ihrer Homepage unter *http://www.dmtf.org/home/*.

WMI-Verbraucher

Ein WMI-Verbraucher (WMI consumer) kann ein Skript, eine Verwaltungsanwendung, eine Webanwendung oder irgendein anderes administratives Tool sein, das auf Verwaltungsinformationen zugreift, die über die WMI-Infrastruktur verfügbar gemacht werden, und sie verändert. Zum Beispiel ist das Skript, das weiter oben in dieser Lektion vorgestellt wurde, um die logischen Festplattenlaufwerke auf Ihrem Computer zu ermitteln und aufzulisten, ein WMI-Verbraucher. Eine Anwendung kann gleichzeitig ein WMI-Anbieter und ein WMI-Verbraucher sein (etwa Microsoft Application Center und Microsoft Operations Manager).

WMI-Skriptingbibliothek

Die WMI-Skriptingbibliothek stellt den Satz Automatisierungsobjekte zur Verfügung, über den Skriptsprachen wie VBScript auf die WMI-Infrastruktur zugreifen. Die WMI-Skriptingbibliothek ist in einem einzelnen Automatisierungsfeature namens *Wbemdisp.dll* implementiert, das im Verzeichnis *SystemRoot\System32\Wbem* gespeichert ist. Die Automatisierungsobjekte in der WMI-Skriptingbibliothek bieten ein konsistentes und einheitliches Skriptingmodell für WMI-verwaltete Ressourcen.



Prüfungstipp

Es ist wichtig, zwischen Klassendefinitionen verwalteter Ressourcen und Automatisierungsobjekten zu unterscheiden. Klassendefinitionen verwalteter Ressourcen liegen im CIM-Repository (*Cim.rep*) und liefern die Baupläne für Computerressourcen, die über WMI verfügbar gemacht werden. Ein allgemeiner Satz Automatisierungsobjekte liegt dagegen in der WMI-Skriptingbibliothek, und Skripts können diese Objekte benutzen, um sich bei WMI zu authentifizieren und eine Verbindung herzustellen. Sobald Sie über die WMI-Skriptingbibliothek eine Instanz einer WMI-verwalteten Ressource abgerufen haben, können Sie mit den Methoden und Eigenschaften darauf zugreifen, die von der Klassendefinition der verwalteten Ressource definiert werden.

Namenskonvention für Variablen

WMI-Skripts folgen bei der Benennung von Variablen üblicherweise einer Konvention. Der Name jeder Variablen leitet sich aus dem Namen des Automatisierungsobjekts in der WMI-Skriptingbibliothek ab, dem `obj` (um deutlich zu machen, dass es sich um einen Objektverweis handelt) oder `col` (für einen Verweis auf ein Auflistungsobjekt, collection object) vorangestellt ist. So heißt eine Variable, die auf ein Objekt namens `SWbemServices` verweist, also `objSWbemServices`. Eine Variable, die auf das Objekt `SWbemObject` verweist, heißt `objSWbemObject`. Und eine Variable, die auf ein Objekt namens `SWbemObjectSet` verweist, bekommt den Namen `colSWbemObjectSet`.

Diese Konvention ist nicht verpflichtend, aber sie hilft zu verstehen, mit welcher Art von WMI-Objekt Sie in einem WMI-Skript arbeiten. Wenn Sie einer einheitlichen Namenskonvention folgen, ist Ihr Code einfacher zu lesen und zu pflegen, vor allem wenn jemand anders später Ihr Skript pflegen muss.

Die WMI-Administrationstools

Sie können die WMI-Administrationstools unter *http://www.microsoft.com/downloads/details.aspx?FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314* herunterladen. Einfacher ist es allerdings, unter *http://www.microsoft.com/downloads* nach »WMI Administrative Tools« zu suchen.

Zu den WMI-Administrationstools gehören:

- **WMI CIM Studio** Hier können Sie Klassen, Eigenschaften, Kennzeichner und Instanzen in einem CIM-Repository ansehen und bearbeiten, ausgewählte Methoden ausführen und MOF-Dateien (Managed Object Format) generieren und kompilieren.
- **WMI Object Browser** Bietet die Möglichkeit, Objekte anzusehen, Eigenschaftswerte und Kennzeichner zu ändern oder Methoden auszuführen.
- **WMI Event Registration Tool** Hier können Sie dauerhafte Ereignisempfänger konfigurieren und Instanzen von Ereignisempfängern, Filtern, Bindungen und Timersystemklassen erstellen oder ansehen.
- **WMI Event Viewer** Zeigt Ereignisse über alle Instanzen registrierter Verbraucher an.

WMI CIM Studio

Das WMI CIM Studio wurde in erster Linie für Entwickler entworfen, vor allem für das Schreiben von Anbietern. Es hilft Entwicklern dabei, WMI-Klassen im CIM-Repository zu erstellen. Das WMI CIM Studio zeigt mithilfe einer Weboberfläche Informationen an und greift auf eine Sammlung von ActiveX-Komponenten zu, die auf dem System installiert werden, wenn das Tool zum ersten Mal ausgeführt wird. Mit dem Tool können Entwickler folgende Arbeiten erledigen:

- Herstellen einer Verbindung zu einem bestimmten System und Durchsuchen der CIM-Repositorys in allen verfügbaren Namespaces
- Suchen nach Klassen anhand ihres Namens, ihrer Beschreibung oder ihrer Eigenschaftsnamen
- Ansehen von Eigenschaften, Methoden und Assoziationen, die zu einer bestimmten Klasse gehören
- Ansehen der Instanzen, die für eine bestimmte Klasse des untersuchten Systems zur Verfügung stehen
- Durchführen von Abfragen in WQL (WMI Query Language)
- Generieren einer MOF-Datei auf Basis ausgewählter Klassen
- Kompilieren einer MOF-Datei, um sie in das CIM-Repository zu laden

Das WMI CIM Studio stellt auch Assistenten bereit, um MOF-Dateien zu generieren und zu kompilieren oder ein Framework für Anbietercode zu erstellen. Wenn Sie das WMI CIM Studio über das Menü *WMI Tools* starten, müssen Sie zuerst in die Informationsleiste klicken und die Ausführung der ActiveX-Tools erlauben. Dann wählen Sie im Dialogfeld *Connect to namespace* einen Namespace aus oder verwenden den Standardnamespace `Root\CIMV2`. Abbildung 13.33 zeigt das WMI CIM Studio.

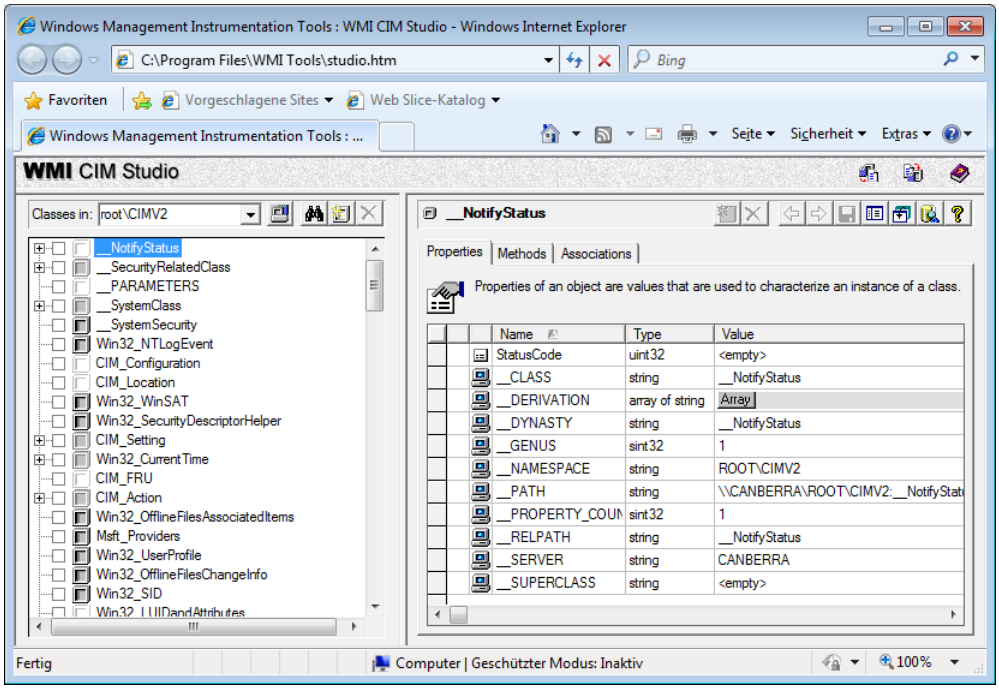


Abbildung 13.33 Das WMI CIM Studio

Das WMI CIM Studio enthält einen Klassenexplorer (Class Explorer) und eine Klassenansicht (Class Viewer). Wenn Sie im Klassenexplorer eine Klasse auswählen, werden ihre Details in der Klassenansicht angezeigt. Die Assistenten von WMI CIM Studio generieren und kompilieren MOF-Dateien.

Sie können sich im WMI CIM Studio die Klassenvererbungsstruktur für alle Namespaces in Ihrem System oder in einem Netzwerk ansehen, indem Sie den Namespacepfad im Feld *Classes in* eingeben, auf das Pfeilsymbol neben *Classes in* klicken und den Namespace in der Liste auswählen oder zu einem Namespace navigieren.

Sie können nach einer bestimmten Klasse im Namespace suchen, indem Sie im Klassenexplorer auf die Schaltfläche *Search for Class* klicken. Aktivieren Sie im Dialogfeld *Search for Class* die gewünschten Kontrollkästchen unter *Search Options*, um festzulegen, welche Art Suche ausgeführt wird: nach Klassenname, Klassenbeschreibung oder Eigenschaftsname. Geben Sie den vollständigen Namen oder einen Ausschnitt ein, nach dem Sie suchen wollen, und klicken Sie auf *Go*. Die Ergebnisse der Suche werden im Fensterabschnitt *Search results* aufgelistet. Wählen Sie die gewünschte Klasse aus und klicken Sie auf *OK*. Daraufhin wird die ausgewählte Klasse im Klassenexplorer angezeigt.

Sie können die Eigenschaften einer Klasse anzeigen, indem Sie sie im Klassenexplorer auswählen und dann in der Klassenansicht auf die Registerkarte *Properties* klicken. Symbole (beispielsweise ein Schlüssel, der für eine Schlüsseleigenschaft steht) liefern auf den ersten Blick folgende Informationen über eine Klasse:

- Schlüsseleigenschaften
- Systemeigenschaften

- Geerbte Eigenschaften
- Änderbare Eigenschaften
- Werte in Eigenschaftsarrays

Sie können im WMI CIM Studio Instanzen einer vorhandenen Klasse anzeigen, indem Sie eine Tabelle aller Instanzen der Klasse öffnen und die Assoziationen einer Instanz anzeigen. Sie können auch benutzerdefinierte Ansichten von Instanzen definieren und anzeigen. Sie können im Klassenexplorer Klassendefinitionen hinzufügen und löschen, und Klassendefinitionen bearbeiten, indem Sie Eigenschaften, Kennzeichner und Methoden hinzufügen, editieren oder löschen. Und Sie können Instanzen einer Klasse hinzufügen und löschen.

Sie können im WMI CIM Studio normale Methoden von Instanzen ausführen, sofern diese Instanzen implementiert und nicht deaktiviert sind. Klicken Sie in der Klassenansicht auf die Klasse und dann auf die Schaltfläche *Instances*. Klicken Sie nun mit der rechten Maustaste auf die Instanz, die Sie bearbeiten wollen, und wählen Sie den Befehl *Go To Object*. Klicken Sie in der Klassenansicht auf die Registerkarte *Methods*, klicken Sie dann mit der rechten Maustaste auf die Methode und wählen Sie den Befehl *Execute Method*. Die Spalte *Parameters* zeigt an, welche Parameter für die Methode definiert sind und welche Standardwerte sie haben. Bevor Sie die Methode ausführen, können Sie die Parameter konfigurieren, indem Sie ihre Werte ändern.

Mit dem WQL Query Builder können Sie WQL-Abfragen schreiben, speichern und ausführen. Klicken Sie dazu in der Klassenansicht auf das Symbol *WQL Queries*. Mit dem Assistenten *MOF Generator* des Klassenexplorers können Sie eine MOF-Datei für Klassendefinitionen und Instanzen aus einem vorhandenen Repository generieren. Üblicherweise führen Sie diesen Assistenten aus, wenn Sie eine neue Klasse angelegt haben oder vorhandene Repositorydaten auf einen anderen Computer exportieren wollen. Sie können außerdem mit dem Assistenten *MOF Compiler* die MOF-Datei in ein Repository kompilieren (das heißt, alle Klassendefinitionen oder Instanzen aus der MOF-Datei in das aktuelle Repository importieren). Dieser Assistent prüft die Syntax einer MOF-Datei und erstellt binäre MOF-Dateien.

WMI Object Browser

Im Unterschied zum WMI CIM Studio ist der WMI Object Browser für Systemverwalter gedacht. In diesem Tool können Sie sich die Objektstruktur für ein CIM-Repository ansehen, Objektdetails anzeigen, Objektdaten bearbeiten und ausgewählte Methoden ausführen. Sie starten den WMI Object Browser über das Menü *WMI Tools*; nach dem ersten Start müssen Sie in die Informationsleiste klicken und die ActiveX-Steuerelemente installieren. Sie können einen Namespace auswählen oder die Standardeinstellung übernehmen.

Der WMI Object Browser enthält einen Objektexplorer (Object Explorer) und eine Objektansicht (Object Viewer). Wenn Sie ein Objekt im Objektexplorer auswählen, werden seine Details in der Objektansicht angezeigt. Abbildung 13.34 zeigt den WMI Object Browser.

Der linke Fensterabschnitt des WMI Object Browsers enthält den Objektexplorer, in dem die Objektstruktur für den aktuellen Namespace angezeigt wird (standardmäßig der Namespace `Root\CIMV2` auf dem lokalen Computer). Sie können einen anderen lokalen Namespace oder einen auf einem Remotecomputer auswählen. Der Objektexplorer zeigt dabei die Hierarchie der Instanzen an, die im ausgewählten Namespace enthalten sind. Sie können jede Instanz aus dem Namespace als Stamm der Strukturansicht auswählen.

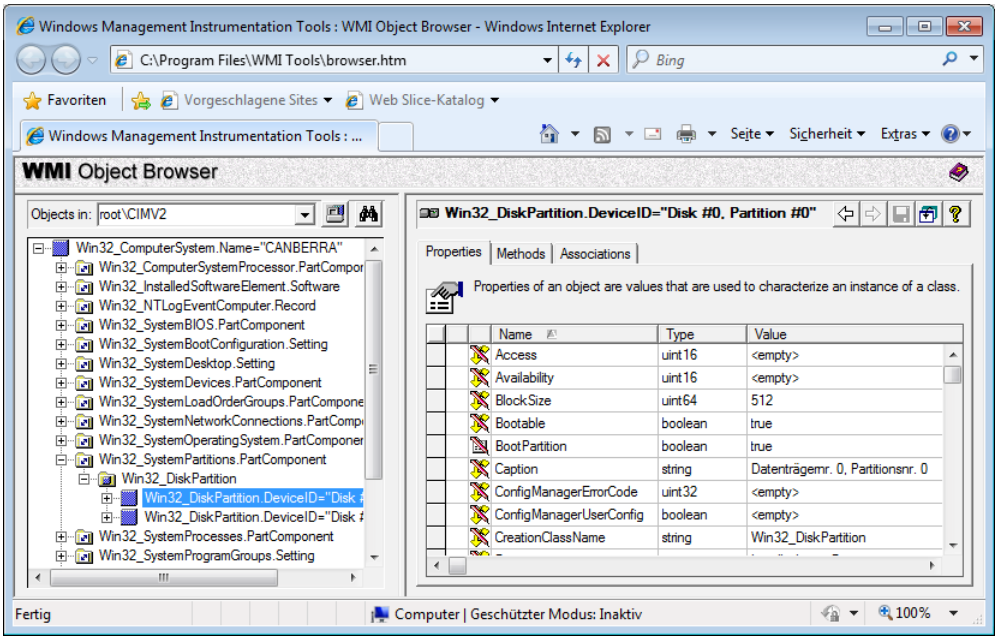


Abbildung 13.34 Der WMI Object Browser

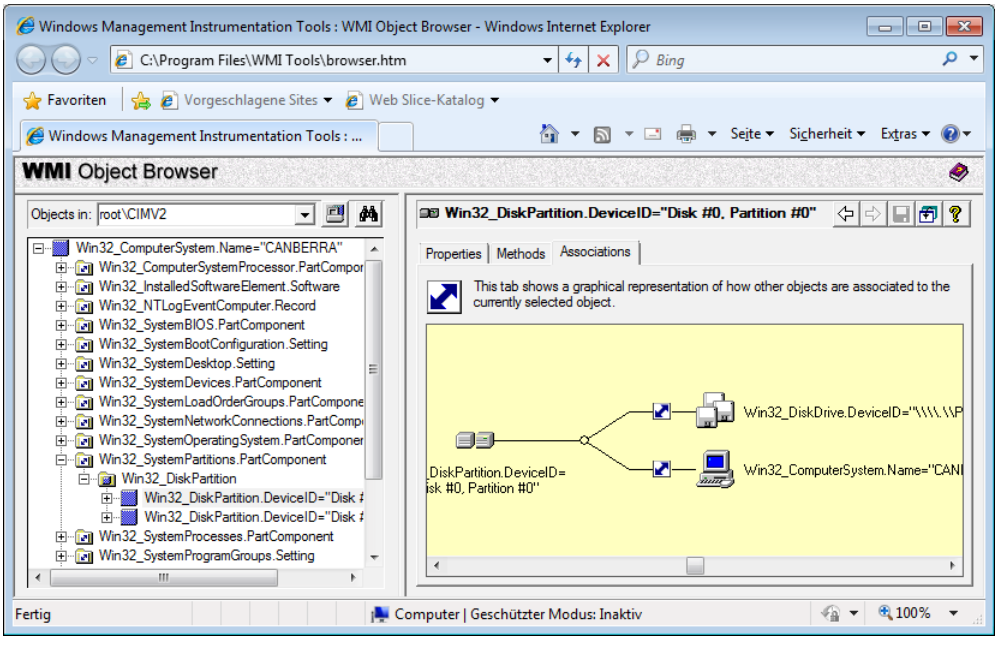


Abbildung 13.35 Die Registerkarte *Associations* im WMI Object Browser

Die Struktur zeigt normale Objekte und Gruppenknoten. Gruppenknoten sind selbst keine Objekte, sie werden vielmehr benutzt, um Objekte zu organisieren. Die Symbole neben den Namen geben den Typ des Objekts beziehungsweise Knotens an. Wenn Sie die Maus über

ein Objekt in der Strukturansicht stellen, wird sein Pfad angezeigt, der das Objekt im Namespace identifiziert.

Der rechte Fensterabschnitt im WMI Object Browser enthält die Objektansicht. Hier können Sie Registerkarten mit den Eigenschaften (*Properties*), Methoden (*Methods*) oder Assoziationen (*Associations*) eines Objekts auswählen. Abbildung 13.35 zeigt die Registerkarte *Associations*. Die Objektansicht zeigt den Titel der aktuellen Ansicht über den Registerkarten an. Bei einem Einzelobjekt ist der Titel der Objektpfad der Instanz, die momentan angezeigt wird. Bei einer Tabelle mit mehreren Objekten beschreibt der Titel die momentan angezeigte Objektgruppe.

Im WMI Object Browser können Sie folgende Aktionen durchführen:

- Anzeigen der Objektstruktur, die im angegebenen CIM-Repository gespeichert ist
- Ändern des Stammobjekts der Objektstruktur
- Anzeigen von Eigenschaften, Methoden und Assoziationen für ein ausgewähltes Objekt
- Anzeigen der Instanzen von Objektgruppen
- Anzeigen von Eigenschafts- und Objektkennzeichnern
- Ausführen von Methoden für ein ausgewähltes Objekt
- Bearbeiten von Eigenschaftswerten sowie Objekt- und Eigenschaftskennzeichnern

Sie können sich die Objektstruktur für alle Namespaces in Ihrem System oder in einem Netzwerk ansehen, indem Sie den Namespacepfad in das Textfeld *Objects in* eingeben oder ihn in der Verlaufsliste auswählen. Sie können auch nach einem Namespace suchen oder mit der rechten Maustaste auf ein Objekt klicken, dessen Namespace Sie anzeigen wollen, und den Befehl *Go To Namespace* wählen. Sie können das Stammobjekt des Namespaces in einer Sitzung vorübergehend ändern. Soll diese Änderung dauerhaft sein, können Sie dafür das Schema anpassen.

Wenn Sie im Objektexplorer einen Gruppenknoten auswählen, zeigt die Objektansicht eine Instanztabelle an, die alle Objekte im Namespace aufführt, die zur ausgewählten Gruppe gehören. Hier werden außerdem die gemeinsamen Eigenschaften dieser Objekte angezeigt. Die Details zu einer ausgewählten Instanz aus der Instanztabelle zeigen Sie an, indem Sie mit der rechten Maustaste auf die Instanz klicken und *Go To Object* wählen. Daraufhin wird die Registerkarte *Properties* des Objekts angezeigt. Auf dieser Registerkarte können Sie doppelt auf eine Eigenschaft klicken, um die Eigenschaftskennzeichner anzuzeigen. Während die Registerkarte *Properties* ausgewählt ist, können Sie mit der rechten Maustaste überall in die Tabelle klicken und den Befehl *Object Qualifiers* wählen. In der Registerkarte *Properties* können Sie außerdem das Wertfeld von Eigenschaften bearbeiten, die nicht schreibgeschützt sind. Sie kehren wieder zur Instanztabelle zurück, indem Sie erneut den Gruppenknoten auswählen.

In der Registerkarte *Methods* der Objektansicht können Sie eine Methode ausführen, indem Sie mit der rechten Maustaste auf eine Methode klicken und den Befehl *Execute Method* wählen. Im Fenster *Parameters* wird angezeigt, welche Parameterwerte übergeben werden, sobald die ausgewählte Methode ausgeführt wird. Die Tabelle *Parameters* führt auf, welche Parameter für die Methode definiert sind und welche Standardwerte sie haben. Um Parameter zu konfigurieren, ändern Sie die Werte in dieser Tabelle, bevor Sie die Methode ausführen.

Das Tool WMI Event Registration

Das Tool *WMI Event Registration* wurde in erster Linie für Entwickler entworfen. Es stellt eine grafische Benutzeroberfläche für Aufgaben bereit, die Sie auch vom Programmcode aus durchführen können. Sie müssen auf dem Zielcomputer die Windows-Verwaltung installieren und ein Repository mit Klassen erstellen, damit Sie das Tool WMI Event Registration benutzen können. Dazu können Sie eine MOF-Datei im Systemverzeichnis kompilieren, in dem der WMI-Kern installiert ist. Geben Sie den folgenden Befehl in einer Eingabeaufforderung ein, um die MOF-Datei zu kompilieren:

```
mofcomp <Dateiname>.mof
```

In der Standardeinstellung verwendet das Tool WMI Event Registration die Datei *Eviewer.mof* aus dem Verzeichnis, in dem die WMI-Tools installiert sind. Diese Datei wird automatisch kompiliert, sobald die Windows-Verwaltung zum ersten Mal startet, daher wird der Verbraucher *WMI Event Viewer* standardmäßig als ständiger Ereignisempfänger registriert. Sie können somit das Tool WMI Event Registration öffnen und seine Features untersuchen.



Weitere Informationen **Kompilieren von MOF-Dateien**

Genauere Informationen darüber, wie Sie MOF-Dateien kompilieren, erhalten Sie, indem Sie das Windows 7 Platform Software Development Kit (SDK) herunterladen und im Abschnitt über WMI (Windows Management Instrumentation) das Thema »Mofcomp« öffnen. Dieses Thema würde allerdings den Rahmen dieses Buchs und der Prüfung 70-680 sprengen.

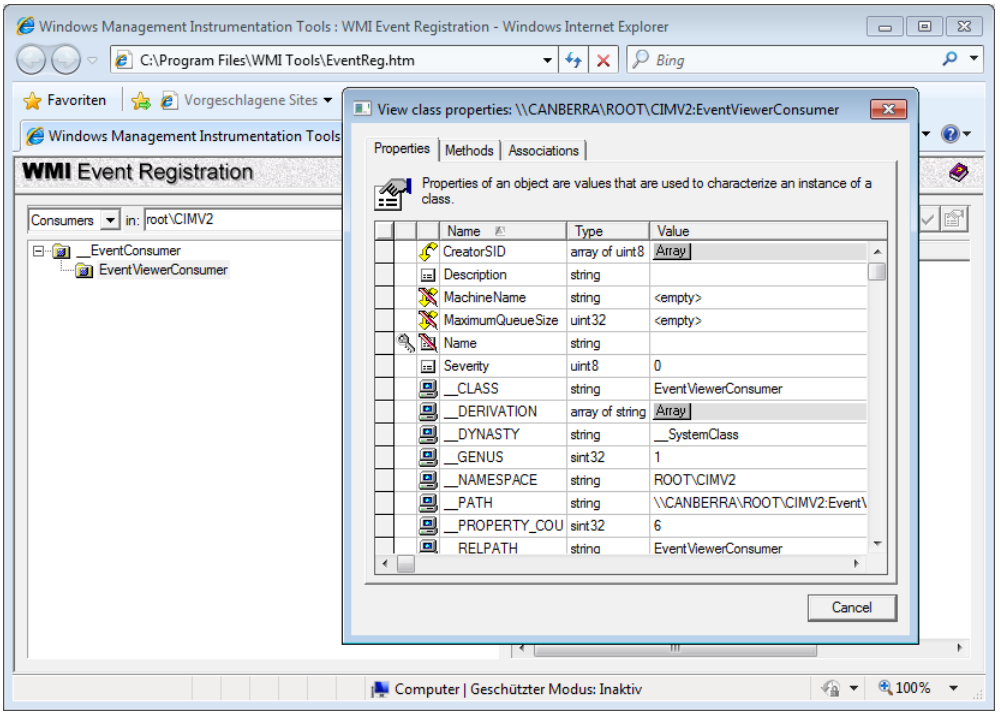


Abbildung 13.36 Das Tool WMI Event Registration

Sie starten das Tool WMI Event Registration im Menü *WMI Tools*. Anschließend müssen Sie, wie bei den anderen Tools, in der Informationsleiste den blockierten ActiveX-Inhalt zulassen und ein Stammverzeichnis angeben. In der Dropdownliste links oben im Fenster haben Sie die Auswahl zwischen Filtern (*Filters*), Verbrauchern (*Consumers*) und Zeitgebern (*Timers*). Wenn Sie ein Element im linken Fensterabschnitt doppelt anklicken, öffnet sich das Dialogfeld *View class properties* (Abbildung 13.36). Hier haben Sie Zugriff auf Registerkarten für Eigenschaften, Methoden und Assoziationen.

Sie können im Tool WMI Event Registration Ereignisempfänger, Filter und Zeitgeber für den ausgewählten Namespace sowie alle Bindungen zwischen Filtern und Verbrauchern erstellen, anzeigen und ändern. In diesem Tool können Sie folgende Aufgaben durchführen:

- Anzeigen der Eigenschaften von definierten Systemklassen und Instanzen für Verbraucher, Filter und Zeitgeber
- Hinzufügen oder Löschen von Ereignisempfängerinstanzen
- Hinzufügen oder Löschen von Ereignisfilterinstanzen
- Hinzufügen oder Löschen von Ereigniszeitgeberinstanzen
- Bearbeiten von Instanzeigenschaften
- Registrieren von Verbrauchern für Ereignisse, indem eine Bindung zwischen Verbraucher und Filter eingerichtet wird

WMI Event Viewer

Der WMI Event Viewer ist ein ständig registrierter Ereignisempfänger, in dem Sie die Details von Ereignissen sortieren und anzeigen können, die in WMI von der Windows-Verwaltung oder Ereignisanbietern generiert werden. Ereignisobjekte werden an alle Verbraucher weitergeleitet, die für den jeweiligen Ereignistyp registriert sind. Sie können den WMI Event Viewer für alle Ereignisfilter registrieren und sich eingehende Ereignisse ansehen, die die Filterkriterien erfüllen.

Sie öffnen den WMI Event Viewer im Menü *WMI Tools*. Als ständig registrierter Ereignisempfänger wird er allerdings von WMI automatisch gestartet, sobald ein Ereignis auftritt, das an ihn weitergeleitet werden muss. Um den WMI Event Viewer für unterschiedliche Ereignistypen zu registrieren, verwenden Sie das Tool WMI Event Registration, das Sie entweder unabhängig im Menü *WMI Tools* oder vom WMI Event Viewer aus starten können, indem Sie auf die Schaltfläche *Register for Events* klicken (Abbildung 13.37).

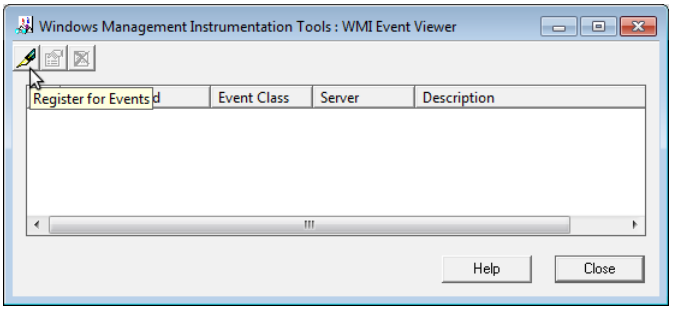


Abbildung 13.37 Die Schaltfläche *Register for Events* im WMI Event Viewer

Im WMI Event Viewer können Sie folgende Aufgaben ausführen:

- Anzeigen von Ereignissen, die von der Windows-Verwaltung generiert werden, und der zugehörigen Ereignisinformationen, darunter Datum und Uhrzeit, Klasse, Herkunft und Beschreibung des Ereignisses
- Anzeigen der Eigenschaften von Ereignisinstanzen
- Starten des Tools WMI Event Registration
- Löschen der Anzeige

Die Datei *Eviewer.mof* wird zusammen mit dem WMI Event Viewer im Verzeichnis der WMI-Tools installiert. Sie enthält die Klassen und Instanzen, die gebraucht werden, um den WMI Event Viewer-Verbraucher beim WMI-Ereignissubsystem zu deklarieren und zu registrieren. Diese MOF-Datei wird automatisch kompiliert, sobald der Dienst *Windows-Verwaltungsinstrumentation* zum ersten Mal gestartet wird. Daher wird der WMI Event Viewer-Verbraucher standardmäßig als ständiger Ereignisempfänger registriert.

Alle ständigen Ereignisempfänger, darunter auch der WMI Event Viewer, benötigen bestimmte DCOM-Berechtigungen (Distributed Component Object Model), wenn sie für ein registriertes Ereignis automatisch auf einem Remotecomputer gestartet werden sollen. Gehen Sie folgendermaßen vor, um die DCOM-Startberechtigungen für den WMI Event Viewer so zu konfigureren, dass Sie Ereignisse auf einem Remotecomputer überwachen können:

1. Starten Sie in einer Eingabeaufforderung mit erhöhten Rechten auf dem Remotecomputer das Programm *Dcomcnfg.exe*.
2. Wählen Sie in der Strukturansicht den Knoten *DCOM-Konfiguration* aus und blättern Sie in der Detailansicht zum Element *WMI Event Viewer* (Abbildung 13.38). Klicken Sie mit der rechten Maustaste auf *WMI Event Viewer* und wählen Sie den Befehl *Eigenschaften*.

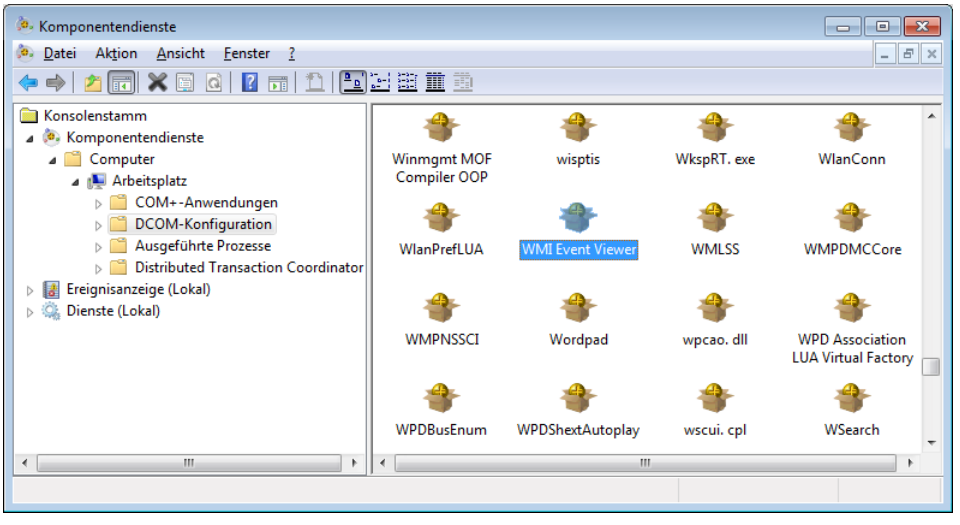


Abbildung 13.38 Auswählen von *WMI Event Viewer* im Fenster *Komponentendienste*

3. Wählen Sie im Dialogfeld *Eigenschaften von WMI Event Viewer* auf der Registerkarte *Sicherheit* im Abschnitt *Start- und Aktivierungsberechtigungen* die Option *Anpassen* aus und klicken Sie auf die zugehörige *Bearbeiten*-Schaltfläche.
4. Klicken Sie auf *Hinzufügen*.
5. Geben Sie im Dialogfeld *Benutzer oder Gruppen auswählen* den Gruppennamen **Jeder** ein und klicken Sie auf *OK*.
6. Aktivieren Sie alle *Zulassen*-Kontrollkästchen für die Gruppe *Jeder* und klicken Sie auf *OK*. Beachten Sie, dass Benutzer und Ereignisempfänger im WMI Event Viewer auf Ereignisinformationen zugreifen können. Es ist kein Konfigurationstool. Daher entstehen keine Sicherheitslücken, wenn Sie diese Berechtigungen einstellen.

Verwenden des Tools *Systemkonfiguration*

Sie öffnen das Tool *Systemkonfiguration* (MSConfig), indem Sie im Suchfeld des Startmenüs, dem Dialogfeld *Ausführen* oder einer Eingabeaufforderung den Befehl **msconfig** eingeben. Dieses Tool dient in erster Linie dazu, Probleme mit dem Startvorgang von Windows zu untersuchen. MSConfig ändert, welche Programme beim Systemstart ausgeführt werden, bearbeitet Konfigurationsdateien und ermöglicht Ihnen, Windows-Dienste zu steuern und auf Windows-Leistungs- und Problembehandlungswerkzeuge zuzugreifen.

Sie können mit dem Tool Systemkonfiguration Windows 7 konfigurieren, um einen Diagnosesystemstart auszuführen, bei dem nur ein Basissatz von Treibern, Programmen und Diensten geladen wird. Abbildung 13.39 zeigt die Registerkarte *Allgemein* des Tools, in der Sie zwischen dem normalen und dem Diagnosesystemstart auswählen. Sie können auch die Option *Benutzerdefinierter Systemstart* auswählen und selbst einstellen, ob Systemdienste und Systemstartelemente geladen werden. Welche Systemdienste und Systemstartelemente dabei geladen und gestartet werden, wählen Sie auf den Registerkarten *Dienste* beziehungsweise *Systemstart* aus.

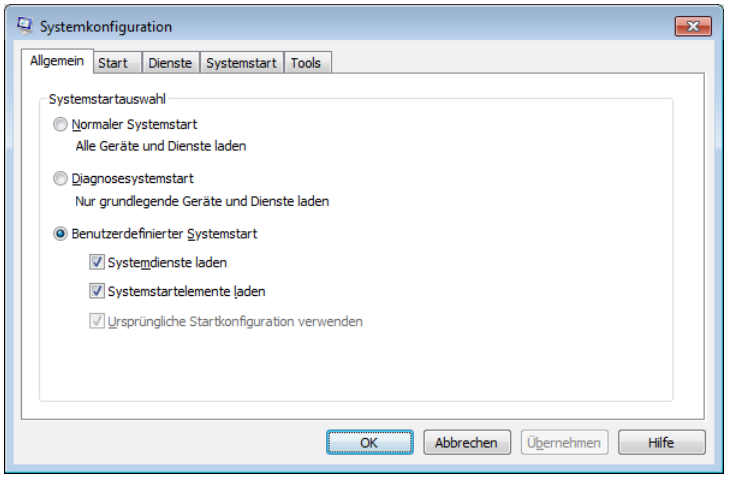


Abbildung 13.39 Die Registerkarte *Allgemein* des Tools *Systemkonfiguration*

Es empfiehlt sich, die Liste der Programme auf der Registerkarte *Systemstart* sorgfältig durchzusehen. Manche Softwarepakete, beispielsweise Programme für die Suche nach Viren und anderer Malware, sollten beim Systemstart ausgeführt werden und ständig laufen, sofern keine zwingenden Gründe vorliegen, sie zu deaktivieren. Andere Softwarepakete, vor allem von anderen Herstellern, installieren sich selbst und starten beim Systemstart, ob sie nun tatsächlich gebraucht werden oder nicht. Je mehr unnötige Programme laufen, desto langsamer wird Ihr Computer.

Dienste sind schwieriger zu verwalten als Pakete, weil Abhängigkeiten zwischen verschiedenen Diensten bestehen. Möglicherweise sehen Sie, dass beim Systemstart ein Dienst ausgeführt wird, von dem Sie noch nie etwas gehört haben, und beschließen, seinen Starttyp zu ändern. Dann müssen Sie aber feststellen, dass ein halbes Dutzend wichtiger Dienste von dem abhängen, den Sie stillgelegt haben. Im Tool *Systemkonfiguration* können Sie mit einem Computer in Ihrem Testnetzwerk experimentieren, bevor Sie derartige Änderungen an Produktivcomputern durchführen.



Hinweis Deaktivieren von Diensten mit MSConfig

Sie können mit MSConfig zwar Dienste deaktivieren, dabei wird aber nicht ihr aktueller Zustand geändert. Zum Beispiel können Sie in MSConfig den laufenden Diagnoserichtliniendienst deaktivieren, aber der Dienst läuft weiter, bis Sie den Computer neu starten.

Auf der Registerkarte *Start* des Tools Systemkonfiguration wählen Sie die Quelle Ihrer Startdateien aus. Wenn Sie wollen, haben Sie die Möglichkeit, eine Quelle zum Standardeintrag zu machen. Beim Computer, dessen Registerkarte *Start* Sie in Abbildung 13.40 sehen, handelt es sich um eine Dual-Boot-Konfiguration, bei der jeweils ein Betriebssystem auf dem Volume *C:* und *D:* liegt. Er kann außerdem Windows 7 Ultimate von einer virtuellen Festplatte (Virtual Hard Disk, VHD) starten. Auf der Registerkarte *Start* können Sie festlegen, wie lange das Systemstartmenü wartet, bis es von der Standardquelle startet.

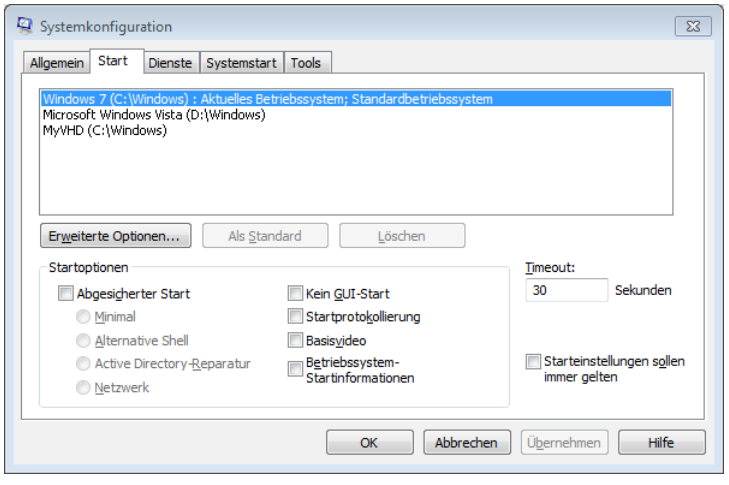


Abbildung 13.40 Die Registerkarte *Start* im Tool *Systemkonfiguration*

Sie können einen abgesicherten Start aktivieren und den zugehörigen Modus einstellen (*Minimal*, *Alternative Shell*, *Active Directory-Reparatur* oder *Netzwerk*). Sie können einen Start ohne grafische Benutzeroberfläche (Graphical User Interface, GUI) ausführen. Wenn Sie Probleme mit einem Grafikkartentreiber haben, können Sie das Kontrollkästchen *Basisvideo* aktivieren, dann wird ein Standardtreiber mit geringer Auflösung und Farbtiefe verwendet. Sie können die Startprotokollierung aktivieren und Informationen zum Betriebssystemstart aufzeichnen lassen. Und Sie können einstellen, ob die geänderten Systemstarteinstellungen nur einmal verwendet werden oder immer gelten sollen.

Wenn Sie auf der Registerkarte *Start* auf *Erweiterte Optionen* klicken, können Sie einen Debugport und die Baudrate für das Remotedebugging auswählen und festlegen, wie viele Prozessoren und welche Arbeitsspeichergröße beim Startprozess höchstens zur Verfügung gestellt wird.

Auf der Registerkarte *Systemstart* können Sie verhindern, dass eine Anwendung automatisch gestartet wird, indem Sie das entsprechende Kontrollkästchen deaktivieren. Wenn Sie auf *Alle deaktivieren* klicken, deaktivieren Sie auf einen Schlag den automatischen Start für alle aufgelisteten Elemente. Dadurch wird die Software nicht beendet: Sie wird lediglich nicht mehr gestartet, wenn Sie den Computer das nächste Mal neu starten. Die Registerkarte *Dienste* funktioniert ganz ähnlich. Sie können hier den automatischen Start eines einzelnen oder aller Dienste deaktivieren oder aktivieren. Sie können auch feststellen, welche Dienste anderer Hersteller laufen, indem Sie das Kontrollkästchen *Alle Microsoft-Dienste ausblenden* ausblenden.

Die Registerkarte *Tools* ist besonders nützlich. Hier sind nicht nur alle verfügbaren Tools aufgelistet, Sie können in dieser Registerkarte auch jedes Tool starten. Das ist oft einfacher, als sich zu merken, wo das Tool in der Systemsteuerung angeordnet ist, ob es ein MMC-Snap-In (Microsoft Management Console) ist oder welche Datei Sie in der Eingabeaufforderung starten müssen, um das Tool auszuführen. Die Registerkarte listet außerdem die ausführbare Datei und den Dateipfad für die Anwendung auf, die jedes Tool ausführt.

Verwenden der Konsole *Dienste*

Die Konsole *Dienste*, ein MMC-Snap-In, listet dieselben Dienste auf wie die Registerkarte *Dienste* im Tool Systemkonfiguration, liefert aber mehr Informationen über jeden Dienst und bietet mehr Möglichkeiten für die Dienstverwaltung. So erfahren Sie in der Konsole *Dienste* unter anderem den Starttyp eines Dienstes (und nicht nur, ob er momentan läuft) und die Anmeldungsdetails.

Sie öffnen die Konsole *Dienste*, indem Sie im Suchfeld des Startmenüs, im Dialogfeld *Ausführen* oder in einem Eingabeaufforderungsfenster **services.msc** eingeben. Sie können die Konsole aber auch in der Registerkarte *Tools* der Systemkonfiguration starten.

Wenn Sie in der Konsole *Dienste* mit der rechten Maustaste auf einen Dienst klicken, bekommen Sie Befehle angeboten, um ihn zu starten, zu beenden, neu zu starten, anzuhalten und fortzusetzen. Sie können außerdem das Eigenschaftendialogfeld für den Dienst öffnen und die Registerkarten *Allgemein*, *Anmelden*, *Wiederherstellung* und *Abhängigkeiten* wählen.

Auf der Registerkarte *Allgemein* legen Sie den Starttyp fest. Zur Auswahl stehen *Automatisch*, *Automatisch (Verzögerter Start)*, *Manuell* und *Deaktiviert*. Beachten Sie folgende Punkte, wenn Sie den Starttyp ändern:

- Ist ein Dienst mit dem Starttyp *Automatisch* konfiguriert, wird er direkt beim Systemstart gestartet. Manche Dienste werden auch automatisch beendet, wenn sie nicht mehr gebraucht werden. Sollten Sie allerdings feststellen, dass Sie einen Dienst nicht brauchen, sollten Sie als Starttyp *Manuell* oder *Deaktiviert* konfigurieren.
- Wenn Sie einen Dienst mit dem Starttyp *Automatisch (Verzögerter Start)* konfigurieren, startet er kurz nach dem Systemstart. Wenn Sie diese Einstellung wählen, beschleunigt sich unter Umständen das Hochfahren des Computers, aber wenn der Dienst während des Systemstarts gebraucht wird, müssen Sie als Starttyp *Automatisch* konfigurieren. Brauchen Sie den Dienst dagegen überhaupt nicht, sollten Sie als Starttyp *Manuell* oder *Deaktiviert* konfigurieren.
- Ist der Starttyp *Manuell* eingestellt, kann Windows 7 den Dienst bei Bedarf starten. In der Praxis kommt es allerdings vor, dass manche Dienste, die mit diesem Starttyp konfiguriert sind, nicht starten, obwohl sie gebraucht werden. Wenn Sie wissen, dass Sie einen Dienst brauchen, sollten Sie als Starttyp *Automatisch* konfigurieren.
- Wenn Sie den Starttyp eines Dienstes als *Deaktiviert* konfigurieren, kann er nicht gestartet werden, selbst wenn er gebraucht wird. Sofern keine zwingenden Gründe vorliegen, einen Dienst zu deaktivieren, sollten Sie als Starttyp stattdessen *Manuell* einstellen.

Auf der Registerkarte *Allgemein* (Abbildung 13.41) erfahren Sie außerdem, ob ein Dienst momentan läuft. Und Sie können ihn starten oder beenden (je nach aktuellem Status) und die Startparameter angeben.

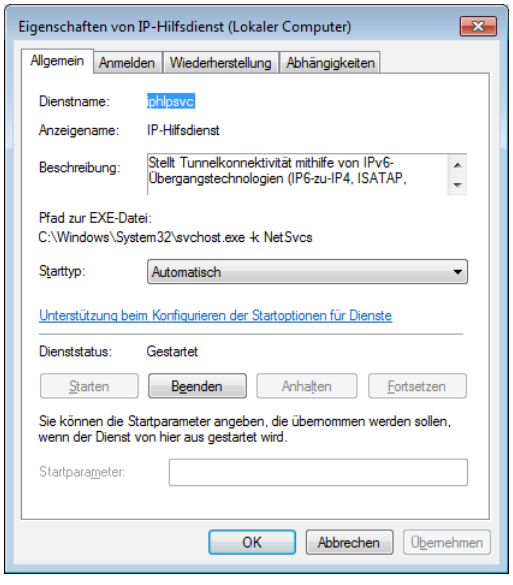


Abbildung 13.41 Die Registerkarte *Allgemein* im Eigenschaftendialogfeld eines Dienstes

Auf der Registerkarte *Anmelden* ist normalerweise festgelegt, dass sich der Dienst unter einem lokalen Systemkonto anmeldet. Sie können bei Bedarf ein anderes Konto angeben, meist ein lokales Administratorkonto auf dem Computer, auf dem der Dienst ausgeführt wird.

Auf der Registerkarte *Wiederherstellung* legen Sie fest, welche Aktionen ausgeführt werden, wenn ein Dienst abstürzt. Sie können Aktionen für den ersten, den zweiten und weitere Fehler konfigurieren.

Wenn Sie den Eintrag *Ein Programm ausführen* auswählen, müssen Sie den vollständigen Pfad des Programms eingeben, das Sie starten wollen. Die hier angegebenen Programme oder Skripts sollten keine Benutzereingabe erfordern. Wenn Sie den Eintrag *Computer neu starten* auswählen, müssen Sie angeben, wie lange der Computer bis zum Neustart wartet. Sie können auch eine Nachricht zusammenstellen, die vor dem Neustart des Computers automatisch an Remotebenutzer gesendet wird.

Wenn Sie das Kontrollkästchen *Aktionen bei Unterbrechungen mit Fehlern aktivieren* auswählen, können Sie festlegen, welche Wiederherstellungsaktionen ausgeführt werden, wenn der Dienst mit einem Fehler abbricht.

Auf der Registerkarte *Abhängigkeiten* sind alle Dienste, Systemtreiber und Startreihenfolgegruppen aufgeführt, die der Dienst benötigt. Falls ein Dienst nicht läuft, obwohl Sie es erwarten, haben Sie unter Umständen einen anderen Dienst deaktiviert, von dem Ihr aktueller Dienst abhängt.

Konfigurieren von Leistungsoptionen

Das Tool *Leistungsoptionen* ist ein Leistungs- und Analysetool in Windows 7. Sie öffnen es, indem Sie im Fenster *Leistungsinformationen und -tools* auf *Weitere Tools* und dann auf *Darstellung und Leistung von Windows anpassen* klicken.

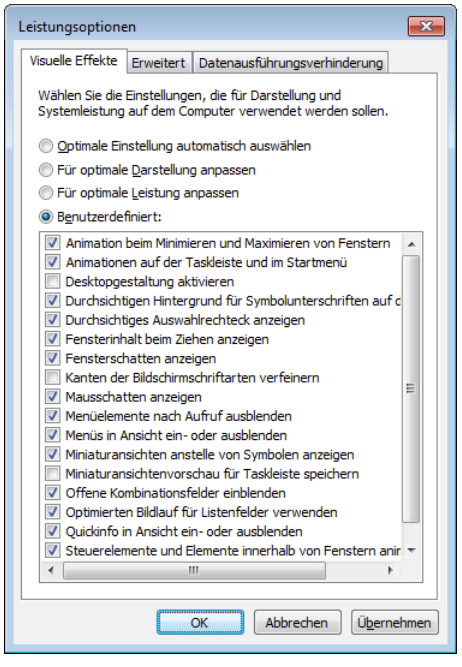


Abbildung 13.42 Die Registerkarte *Visuelle Effekte* im Tool *Leistungsoptionen*

Abbildung 13.42 zeigt die Registerkarte *Visuelle Effekte* des Tools. Sie können die optimale Einstellungen von Windows wählen lassen, optimale Darstellung oder optimale Leistung konfigurieren oder *Benutzerdefiniert* auswählen und die einzelnen Darstellungseinstellungen für Ihren Computer selbst auswählen. Wenn Sie die Option *Benutzerdefiniert* verwenden, können Sie individuell einstellen, welche visuellen Effekte ein- und ausgeschaltet werden. Es gibt 18 visuelle Effekte, die Sie steuern können. Hier haben Sie beispielsweise die Auswahl, ob Schatten unter Bildschirmsymbolen oder dem Mauszeiger angezeigt werden.

Auf der Registerkarte *Erweitert* können Sie Einstellungen vornehmen, die sich auf die Leistung von Programmen oder Hintergrunddiensten auswirken. Wenn Ihr Computer Anwendungen ausführt (wie die meisten Arbeitsstationen), sollten Sie unter *Optimale Leistung anpassen für* die Option *Programme* auswählen. Auf einem Server, der beispielsweise als Webserver eingesetzt wird, sollten Sie unter *Optimale Leistung anpassen für* stattdessen die Option *Hintergrunddienste* wählen.

Auf derselben Registerkarte können Sie auch Einstellungen für die Auslagerungsdateien konfigurieren. Eine Auslagerungsdatei (page file) ist ein Bereich auf der Festplatte, in den virtueller Arbeitsspeicher ausgelagert werden kann, während arbeitsspeicherintensive Operationen (etwa Druckerspooling) laufen oder das System-RAM nicht für die laufenden Anwendungen ausreicht. Sie können es Windows 7 überlassen, die Auslagerung des Arbeitsspeichers zu verwalten (Standardeinstellung), wie in Abbildung 13.43 gezeigt. Oder Sie legen die Zuweisung von virtuellem Arbeitsspeicher selbst fest. Sofern das RAM ein ernster Leistungsengpass auf Ihrem Computer ist oder Sie besonders arbeitsspeicherintensive Anwendungen ausführen, ist es unter Umständen sinnvoll, die Einstellungen für die Auslagerungsdateien von Hand zu konfigurieren. Andernfalls sollten Sie die Standardeinstellung verwenden.

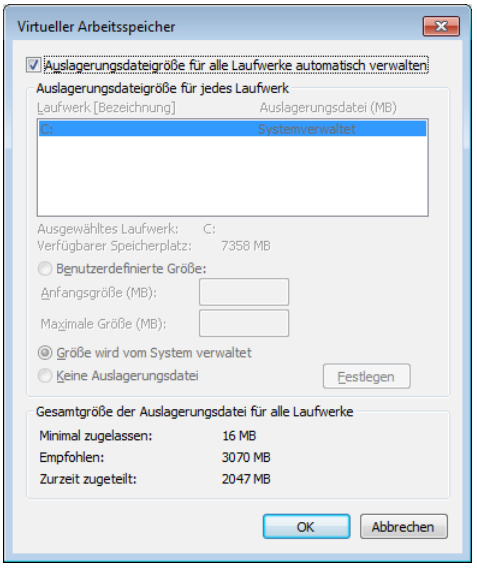


Abbildung 13.43 Standardeinstellungen für virtuellen Arbeitsspeicher

Die Datenausführungsverhinderung (Data Execution Prevention, DEP) hilft dabei, Schäden an Ihrem Computer aufgrund von Viren und anderen Sicherheitsbedrohungen einzudämmen. Malwareangriffe auf Ihr Betriebssystem versuchen, Code aus Abschnitten im Arbeitsspeicher des Computers auszuführen, der für Windows 7 und andere autorisierte Programme reserviert ist. DEP hilft beim Schutz Ihres Computers, indem es Programme überwacht und sicherstellt, dass sie den Arbeitsspeicher des Computers auf sichere Weise benutzen. Erkennt DEP, dass ein Programm auf Ihrem Computer versucht, den Arbeitsspeicher in falscher Weise zu nutzen, schließt sie das Programm und benachrichtigt Sie.

Auf der Registerkarte *Datenausführungsverhinderung* im Tool Leistungsoptionen stellen Sie ein, ob DEP ausschließlich für wichtige Windows-Programme und Dienste (Standardeinstellung) oder für alle Programme und Dienste außer den explizit angegebenen aktiviert wird. In einer Testumgebung, wo Entwickler Anwendungen testen, die versehentlich Sicherheitsprobleme auf dem Computer verursachen könnten, ist es sinnvoll, DEP für alle Programme und Dienste zu erzwingen. Dabei können Sie bei Bedarf Ausnahmen für Anwendungen festlegen, denen Sie vollständig vertrauen.

Konfigurieren des Schreibcaches für Festplatten

Der Schreibcache verwendet schnelles RAM, um Schreibbefehle, die Daten an Speichergeräte senden, zu sammeln und zwischenzuspeichern, bis das langsamere Speichermedium (Festplatten oder Flashspeicher) sie verarbeiten kann. Sie verwalten den Schreibcache auf der Registerkarte *Richtlinien* im Eigenschaftendialogfeld eines Geräts, das Sie im Geräte-Manager öffnen.

Bei Geräten wie USB-Flashsticks können Sie die Option *Schnelles Entfernen* auswählen (Abbildung 13.44). Sie eignet sich am besten für Geräte, die häufig vom System abgezogen werden, wie beispielsweise USB-Flashlaufwerke, Speicherkarten oder andere extern angeschlossene Speichergeräte.

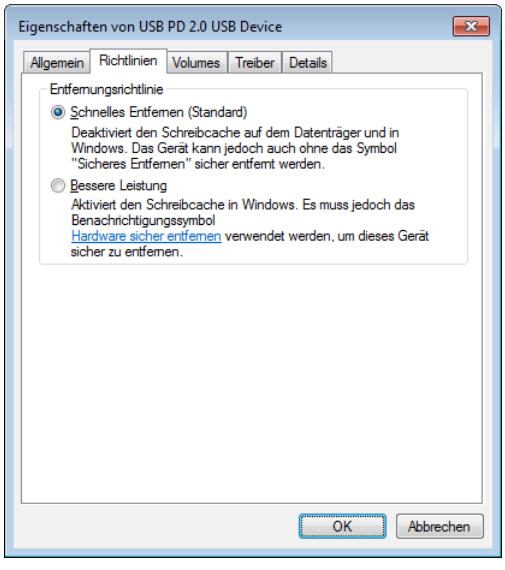

Eigenschaften von USB PD 2.0 USB Device
Allgemein
Richtlinien
Volumes
Treiber
Details
Entfernungsrichtlinie
Schnelles Entfernen (Standard)
Deaktiviert den Schreibcache auf dem Datenträger und in Windows. Das Gerät kann jedoch auch ohne das Symbol "Sicheres Entfernen" sicher entfernt werden.
Bessere Leistung
Aktiviert den Schreibcache in Windows. Es muss jedoch das Benachrichtigungssymbol
Hardware sicher entfernen verwendet werden, um dieses Gerät sicher zu entfernen.
OK
Abbrechen

Abbildung 13.44 Die Option *Schnelles Entfernen* für Wechselmedien

Wenn Sie die Option *Schnelles Entfernen* einstellen, verwaltet Windows 7 die Befehle, die an das Gerät gesendet werden, mit einem sogenannten Write-Through-Cache. Bei dieser Methode arbeitet das Gerät bei Schreibbefehlen so, als gäbe es keinen Cache. Der Cache bietet unter Umständen einen leichten Leistungsgewinn, aber in erster Linie sollen die Daten so sicher wie möglich sein. Dies hat vor allem den Vorteil, dass Sie das Speichergerät schnell vom System abziehen können, ohne Datenverlust zu riskieren. Wird zum Beispiel ein Flashlaufwerk versehentlich aus dem USB-Anschluss gezogen, ist die Gefahr, dass geschriebene Daten verloren gehen, viel geringer, wenn die Option *Schnelles Entfernen* ausgewählt ist.

Die Option *Bessere Leistung* sollten Sie für Geräte verwenden, die nur selten vom System entfernt werden. Wenn diese Option ausgewählt ist und das Gerät vom System abgezogen wird, bevor alle Daten geschrieben wurden (weil Sie beispielsweise ein USB-Flashlaufwerk vorzeitig abziehen), besteht die Gefahr, dass Daten verloren gehen.

Wenn Sie bei einer Festplatte das Kontrollkästchen *Schreibcache auf dem Gerät aktivieren* (Standardwert) aktivieren, verbessert das die Systemleistung, aber bei einem Stromausfall oder Systemfehler kann Datenverlust auftreten. In der Standardeinstellung leert Windows 7 den Cache regelmäßig und weist das Speichergerät an, alle Daten, die im Cache liegen, auf das Speichermedium zu übertragen. Wenn Sie das Kontrollkästchen *Leeren des Windows-Schreibcachepuffers auf dem Gerät deaktivieren* aktivieren, werden diese regelmäßigen Datenübertragungsbefehle unterbunden. Nicht alle Festplatten unterstützen dieses Feature. Abbildung 13.45 zeigt die Karte *Richtlinien* im Eigenschaftendialogfeld einer Festplatte.

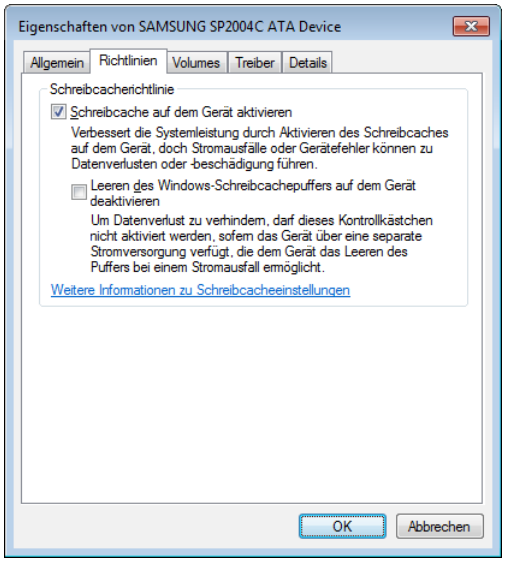

Eigenschaften von SAMSUNG SP2004C ATA Device
Allgemein
Richtlinien
Volumes
Treiber
Details
Schreibcacherichtlinie
Schreibcache auf dem Gerät aktivieren
Verbessert die Systemleistung durch Aktivieren des Schreibcaches auf dem Gerät, doch Stromausfälle oder Gerätefehler können zu Datenverlusten oder -beschädigung führen.
Leeren des Windows-Schreibcachepuffers auf dem Gerät deaktivieren
Um Datenverlust zu verhindern, darf dieses Kontrollkästchen nicht aktiviert werden, sofern das Gerät über eine separate Stromversorgung verfügt, die dem Gerät das Leeren des Puffers bei einem Stromausfall ermöglicht.
Weitere Informationen zu Schreibcacheeinstellungen
OK
Abbrechen

Abbildung 13.45 Die Registerkarte *Richtlinien* bei einer Festplatte

Wenn Sie vor allem auf eine hohe Datenübertragungsleistung abzielen, sollten Sie für Wechselmedien die Option *Bessere Leistung* und für Festplatten das Kontrollkästchen *Schreibcache auf dem Gerät aktivieren* auswählen. Dies sind auch die Standardeinstellungen, sofern Systemhardware und Speichergerät diese Features unterstützen. Wenn allerdings öfter Probleme mit Ihrem System oder der Stromversorgung auftreten, sollten Sie diese Einstellungen nicht verwenden. Ohnehin sollten Sie generell das Applet *Hardware sicher entfernen* verwenden, bevor Sie ein externes Speichergerät von Ihrem System abziehen.

Untersuchen von Leistungsproblemen mit der Ereignisanzeige

Als IT-Experte müssen Sie gelegentlich Details zu Software- und Hardwareproblemen untersuchen, unter denen die Windows-Leistung leidet. Sie können sich Ereignisprotokolle in der Ereignisanzeige ansehen, wie in Lektion 1 dieses Kapitels beschrieben, und die Einträge anhand des Ereignistyps filtern. Im Allgemeinen interessieren Sie sich in diesem Zusammenhang für Ereignisse im Container *Betriebsbereit* unter *Diagnostics-Performance*. Erweitern Sie dazu in der Konsolenstruktur der Ereignisanzeige die Knoten *Anwendungs- und Dienstprotokolle*, dann *Microsoft* und schließlich *Windows*.

Es gibt aber auch eine simplere Methode, diese Informationen abzurufen: Klicken Sie in der Systemsteuerung auf das Element *Leistungsinformationen und -tools*, dann auf *Weitere Tools* und schließlich auf *Leistungsdetails im Ereignisprotokoll anzeigen*. Daraufhin öffnet sich die Ereignisanzeige und zeigt die Ereignisse im Container *Betriebsbereit* an. In Abbildung 13.46 weist beispielsweise ein kritischer Fehler darauf hin, dass beim Computer *Canberra* ein Problem während des Startprozesses auftrat.

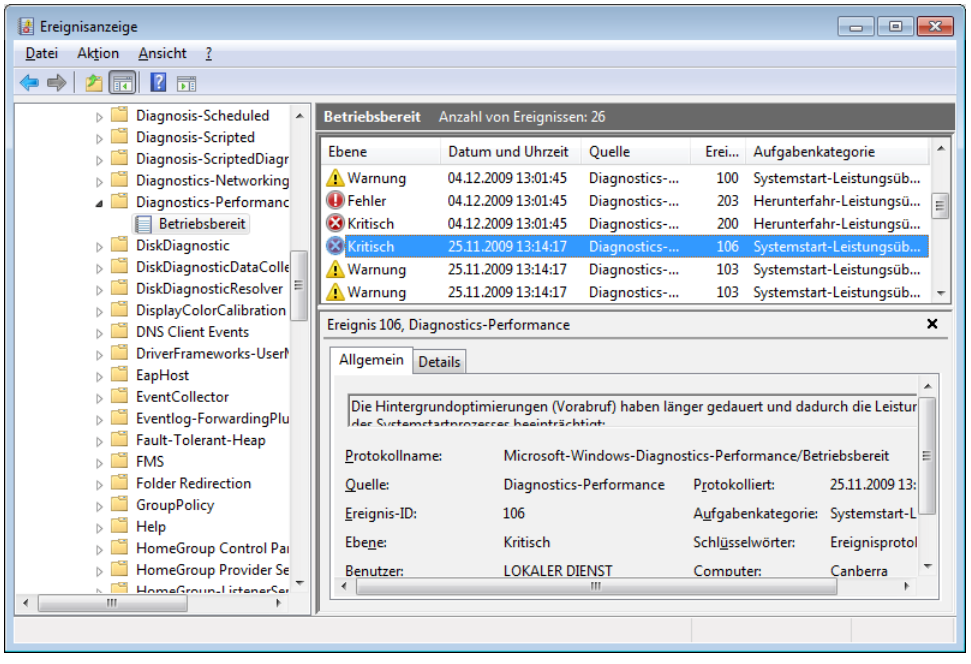


Abbildung 13.46 Anzeigen von Leistungsdiagnoseereignissen im Container *Betriebsbereit*



Hinweis Gerätetreiber

Funktioniert ein Gerät nicht richtig, wirkt sich das oft katastrophal auf die Leistung aus. Sie müssen sicherstellen, dass für alle Ihre Geräte (normalerweise) die neusten Gerätetreiber installiert sind. Eine Ausnahme ist der Fall, dass ein neuer Gerätetreiber schlechter arbeitet als sein Vorgänger. Dann sollten Sie die Vorversion des Gerätetreibers wiederherstellen. Kapitel 4, »Verwalten von Geräten und Datenträgern«, beschreibt dieses Thema genauer.



Hinweis Energiesparpläne

Energiesparpläne und das Konfigurieren von Energieeinstellungen sind in den Prüfungszielen erwähnt, die von diesem Kapitel abgedeckt werden. Aber Kapitel 11, »BitLocker und Mobilitätsoptionen«, beschreibt diese Themen ausführlich, daher besteht kein Grund, hier noch einmal darauf einzugehen.

Konfigurieren von Prozessen im Task-Manager

Lektion 1 hat beschrieben, wie Sie im Task-Manager abgestürzte Anwendungen schließen und Dienste verwalten. Sie können mit diesem Tool aber auch die Prozesse konfigurieren, von denen Dienste implementiert werden. Wenn ein Prozess besonders wichtig ist und er mehr Ressourcen bekommen sollte, können Sie eine höhere Priorität dafür festlegen. Verbraucht ein Prozess zu viele Ressourcen oder ist es egal, wie schnell ein Prozess läuft, können Sie ihm eine niedrigere Priorität zuweisen und dadurch Ressourcen für andere Prozesse freimachen.

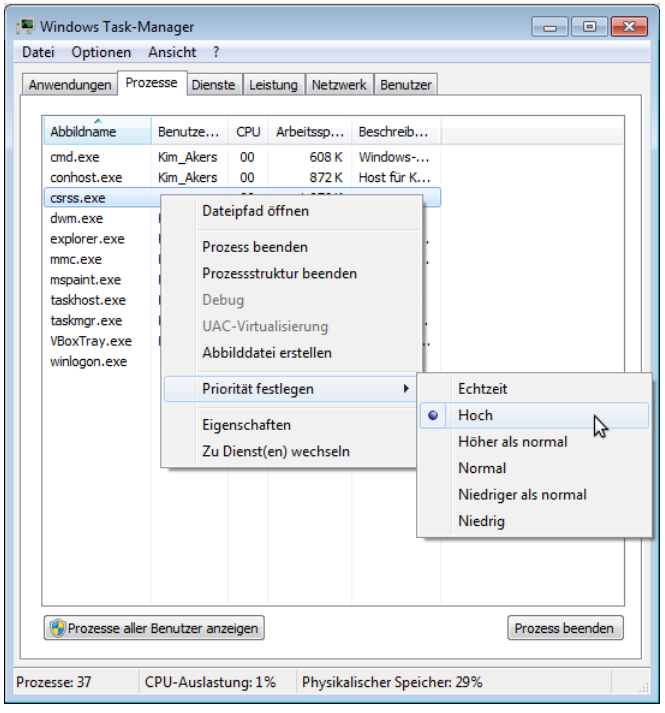


Abbildung 13.47 Einstellen der Prozesspriorität im Task-Manager

Wenn Ihr Computer mehrere Prozessoren hat, können Sie die Zugehörigkeit (affinity) Ihrer Prozesse konfigurieren, sodass sie einen bestimmten Prozessor benutzen. In der Standardeinstellung sind Prozesse, die auf einem Computer mit mehreren Prozessoren installiert werden, so eingestellt, dass sie irgendeinen freien Prozessor verwenden. Wird allerdings nachträglich ein weiterer Prozessor in einen Computer eingebaut, müssen Sie unter Umständen die Konfiguration von Prozessen ändern, damit sie auch den neuen Prozessor nutzen. Zeigen Task-Manager oder Leistungsüberwachungsindikatoren beispielsweise, dass in

einem Computer, der 2 Prozessoren hat, der eine Prozessor stark ausgelastet ist, der andere aber kaum etwas zu tun hat, sollten Sie die Zugehörigkeit so ändern, dass ressourcenintensive Prozesse beide Prozessoren benutzen. Sie haben auch die Möglichkeit, die Zugehörigkeit einiger Prozesse so einzustellen, dass sie nur den zweiten Prozessor verwenden.

Um zu ermitteln, welche Prozesse von einem Dienst benutzt werden, klicken Sie auf der Registerkarte *Dienste* des Task-Managers mit der rechten Maustaste auf den gewünschten Dienst und wählen den Befehl *Zu Prozess wechseln*. Daraufhin wechselt das Tool zur Registerkarte *Prozesse*, wo der zugehörige Prozess ausgewählt ist. Sie ändern die Priorität eines Prozesses, indem Sie ihn mit der rechten Maustaste anklicken und das Untermenü *Priorität festlegen* auswählen. Nun haben Sie die Wahl zwischen sechs Prioritätsstufen (Abbildung 13.47). Wählen Sie aber nicht *Echtzeit* aus, denn das könnte die Ausführung anderer Prozesse auf Ihrem Computer empfindlich stören.

Wenn Sie die Zugehörigkeit eines Prozesses ermitteln oder ändern wollen, können Sie mit der rechten Maustaste auf den Prozess klicken und den Befehl *Zugehörigkeit festlegen* wählen. Es ist nicht möglich, die Zugehörigkeit bestimmter Systemprozesse zu ändern. Und wenn der Computer nur einen Prozessor hat, können Sie die Zugehörigkeit natürlich auch nicht einstellen. Andernfalls öffnet sich das Dialogfeld *Prozessorzugehörigkeit*, wo Sie konfigurieren, auf welchen Prozessoren ein Prozess ausgeführt wird (Abbildung 13.48).

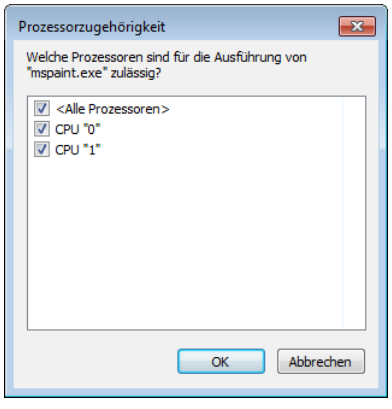


Abbildung 13.48 Das Dialogfeld *Prozessorzugehörigkeit*

Konfigurieren der Netzwerkleistung

Die Netzwerkleistung in einem großen Unternehmensnetzwerk hängt von sehr vielen Faktoren ab, darunter dem Typ der benutzten Ethernet- oder Drahtlosverbindungen, der Geschwindigkeit von Switches und Routern und der Zahl der Geräte in einem Netzwerk. In einem kleinen Netzwerk neigen die Benutzer dazu, die Netzwerkleistung danach zu beurteilen, wie schnell die Verbindung zu anderen Computern im Netzwerk (beim Übertragen von Dateien) und die Internetverbindung sind.

Wenn Sie die Internetoptionen konfigurieren, kann das deutliche Auswirkungen auf die Netzwerkleistung im Besonderen und die Gesamtleistung des Computers im Allgemeinen haben. Als IT-Experte wissen Sie, dass temporäre Internetdateien viel Platz auf der Festplatte belegen können und regelmäßig gelöscht werden sollten. Sie wissen, dass bei Benutzern, die besonders große Postfächer haben, die Anmeldung recht lange dauern kann, vor allem wenn

sie ihr Profil von einem zentralen Server in der Unternehmensumgebung herunterladen. Das sind allerdings Probleme, die sich eher über Benutzerschulung als die Konfiguration lösen lassen.

Das Dialogfeld *Eigenschaften von Internet* enthält Konfigurationsoptionen, die sich auf die Netzwerkleistung auswirken. Sie können dieses Dialogfeld in der Systemsteuerung unter *Netzwerk und Internet* oder von Ihrem Browser aus öffnen. Auf der Registerkarte *Allgemein* können Sie temporäre Internetdateien und andere heruntergeladene Daten löschen, beispielsweise Daten aus Webformularen. Im Zusammenhang mit der Netzwerkleistung ist allerdings die Registerkarte *Erweitert* dieses Dialogfelds am wichtigsten (Abbildung 13.49).

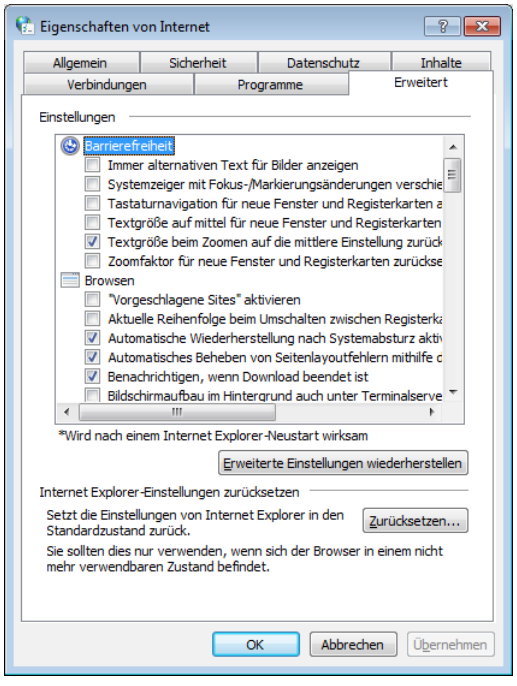


Abbildung 13.49 Die Registerkarte *Erweitert* im Dialogfeld *Eigenschaften von Internet*

Auf der Registerkarte *Erweitert* konfigurieren Sie Einstellungen aus den Bereichen Barrierefreiheit, Browsen, International, Multimedia, Drucken und Sicherheit. Einige davon haben kaum oder gar keine Auswirkungen auf die Leistung, andere sind für die Leistung sehr wichtig. So denken Sie wahrscheinlich, dass die Features aus dem Bereich *Barrierefreiheit* im Zusammenhang mit der Leistung unwichtig sind. Aber wenn für einen Benutzer, der das gar nicht braucht, eine große Schriftart oder Fokusänderungen eingestellt sind, hat dieser Benutzer den Eindruck, dass sich die Leistung verschlechtert.

Die Einstellungen aus dem Bereich *Browsen* können sich auf die Leistung auswirken. Wenn Sie beispielsweise das Skriptdebuggen nicht deaktivieren und Benachrichtigungen über Skriptfehler anzeigen, wird der Benutzer beim Browsen behindert. Diese Einstellungen sind nützlich, während Sie eine neue Website debuggen, die Skripts ausführt. Für den Standardbenutzer sind sie aber fehl am Platz. Selbst vermeintlich simple Einstellungen wie das Unter-

streichen von Links können das Browsen auf langsamen oder stark ausgelasteten Sites verlangsamen.

Wenn Sie auf Sites zugreifen, die Multimediadateien als Streams oder Download zur Verfügung stellen, können Sie (unter anderem) auswählen, ob Audio und Animationen abgespielt, die Größe von Bildern automatisch angepasst oder Platzhalter beim Bilderdownload angezeigt werden. Effekte, die Multimediaelemente verschönern, machen Zugriffe auf eine Site im Allgemeinen langsamer.

Je sicherer eine Site ist, desto langsamer ist sie üblicherweise, weil zusätzliche Sicherheitsprüfungen durchgeführt werden. Das ist etwas, was Sie und Ihre Benutzer im Allgemeinen schlicht in Kauf nehmen müssen. Sie sollten die Sicherheit nicht verringern, nur um die Zugriffszeiten ein wenig zu verkürzen. Allerdings ist es wahrscheinlich nicht nötig, Benutzer jedes Mal zu warnen, wenn sie von einer sicheren HTTPS-Site auf eine unsichere HTTP-Site wechseln.

Windows-Leistungsanalysetools

Das Windows Performance Toolkit (WPT) enthält Leistungsanalysetools, die im Windows SDK für Windows 7, Windows Server 2008 und Microsoft .NET Framework 3.5 neu eingeführt wurden. Das WPT eignet sich für eine Vielzahl von IT-Experten, etwa Systemadministratoren, Netzwerkadministratoren und Anwendungsentwickler. Die Tools wurden entworfen, um die System- und Anwendungsleistung auf Windows Vista, Windows Server 2008, Windows Server 2008 R2 und Windows 7 zu messen und zu analysieren.

Die Windows-Leistungsanalysetools analysieren eine Vielzahl von Leistungsproblemen, darunter Anwendungsstartzeiten, Systemstartprobleme, DPCs (Deferred Procedure Call), ISRs (Interrupt Service Request), Probleme mit der Systemreaktionszeit, Auslastung von Anwendungsressourcen und Interruptwellen.

Diese Tools sind im Microsoft Windows SDK für Windows 7 und .NET Framework 3.5 SP1 enthalten, das Sie von *http://www.microsoft.com/downloads/details.aspx?familyid=C17BA869-9671-4330-A63E-1FD44E0E2505* herunterladen können. (Wahrscheinlich ist es allerdings einfacher, wenn Sie im Microsoft Download Center unter *http://www.microsoft.com/downloads* nach dem SDK suchen). Dieses SDK enthält Dokumentation, Beispiele, Headerdateien, Bibliotheken und Tools, die Sie brauchen, um Anwendungen für Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2, Windows 7, und die .NET Framework-Versionen 2.0, 3.0 und 3.5 zu entwickeln. In den Übungen weiter unten in dieser Lektion laden Sie das SDK herunter und installieren es.

Das WPT ist als MSI-Installationsdatei (eine pro Architektur) im SDK enthalten. Die Leistungsanalysetools sind Teil des WPTs, sie umfassen folgende Tools:

- **Trace Capture, Processing, and Command-Line Analysis Tool (*Xperf.exe*)** Dieses Tool zeichnet Ablaufverfolgungen auf, verarbeitet sie für die Auswertung auf einem Computer und unterstützt die Ablaufverfolgungsanalyse in der Befehlszeile (aktionsbasiert).
- **Visual Trace Analysis Tool (*Xperfview.exe*)** Dieses Tool stellt Ablaufverfolgungsinhalt in Form von interaktiven Diagrammen und Übersichtstabellen dar.
- **On/Off Transition Trace Capture Tool (*Xbootmgr.exe*)** Dieses Tool automatisiert An/Aus-Statusübergänge und zeichnet während solcher Übergänge Ablaufverfolgungen auf.

Trace Capture, Processing, and Command-Line Analysis Tool

Xperf.exe ist ein Befehlszeilentool, das folgende Features aufweist:

- Ereignisablaufverfolgung für die Windows-Ablaufverfolgungssteuerung (Event Tracing for Windows, ETW)
- Zusammenführen und Verbessern von ETW-Ablaufverfolgungen durch Einarbeiten anderer Ereignisse
- Ausführbare Abbild- und Symbolidentifizierung
- Ablaufverfolgungsspeicherung
- Unterstützung für Nachbearbeitung

Dieses Tool verwaltet die Endpunkt-zu-Endpunkt-Operationen, die nötig sind, um eine Ablaufverfolgungsdatei für Analysezwecke zu generieren. Sie benutzen *Xperf.exe* in den Übungen weiter unten in dieser Lektion.

Xperf.exe aktiviert Ereignisse im Betriebssystem mithilfe von Gruppen und Flags. Diese Flags aktivieren oder deaktivieren Ereignisse von Anbietern in verschiedenen Teilen des Betriebssystems. Beispielsweise können Flags den Kernel, Dienste und Anwendungen auf eine oder mehrere Ablaufverfolgungsdateien verweisen, wobei Protokollsitzungen mit benutzerdefinierter Konfiguration verwendet werden. Sie können dann alle Ablaufverfolgungen in einer einzigen Ablaufverfolgungsdatei zusammenführen. Diese Datei wird als zusammengeführte Ablaufverfolgungsdatei (merged trace file) bezeichnet.

Wenn Xperf diese Datei generiert, sammelt es zusätzliche Informationen über das Betriebssystem und fügt sie zur zusammengefassten Ablaufverfolgung hinzu. Sie können die zusammengefasste Ablaufverfolgungsdatei in jedem unterstützten Betriebssystem verarbeiten, es braucht nicht dasselbe System zu sein wie das, auf dem die Ablaufverfolgung generiert wurde. Anschließend können Sie die zusammengefasste Datei mit dem Performance Analyzer (*Xperfview.exe*) analysieren, die zusammengefasste Datei in einer Textdatei nachbearbeiten oder mithilfe von Aktionen (action) andere Verarbeitungsmethoden ausführen. Aktionen erstellen zusammengefasste Ausgaben, die für einen ausgewählten Bereich von Bedeutung sind, etwa Systemstart, Herunterfahren, Wechseln in den Ruhezustand oder Aufwecken des Computers, oder die sich auf andere Arten von Systemereignissen konzentrieren, zum Beispiel Profilaufzeichnung, Kontextumschaltung, DPCs und ISRs, Datenträger-E/A, Registrierungszugriffe, Dateizugriffe oder Systemkonfiguration.

Visual Trace Analysis Tool

Das Visual Trace Analysis Tool, auch Performance Analyzer genannt, zeigt Informationen aus einer einzigen Ablaufverfolgungsdatei an, die von *Xperf.exe* generiert wurde. Sie starten den Performance Analyzer mit folgendem Befehl:

```
xperf <Datei>.etl
```

Xperf.exe leitet den Dateinamen an den Performance Analyzer weiter, der daraufhin die Datei öffnet und ihre Daten anzeigt. Sie können den Performance Analyzer auch direkt ausführen, indem Sie im Suchfeld des Startmenüs, im Dialogfeld *Ausführen* oder in einer Eingabeaufforderung **xperfview** eingeben. In den Übungen weiter unten in dieser Lektion finden Sie eine Abbildung, die zeigt, wie eine Ablaufverfolgung im Performance Analyzer dargestellt wird.

On/Off Transition Trace Capture Tool

Xbootmgr.exe sammelt Informationen während der Ein/Aus-Umschaltphasen von Windows 7. Sie können Daten während der folgenden Phasen aufzeichnen:

- Systemstart
- Herunterfahren
- Umschalten in den Standbymodus und Aufwecken des Computers
- Umschalten in den Ruhezustand und Aufwecken des Computers

Nachdem Sie einen Ablaufverfolgungsbefehl ausgeführt haben, wird der Testcomputer innerhalb von 5 Sekunden zurückgesetzt.

Das On/Off Transition Trace Capture Tool kann einen Neustartzyklus automatisieren, bei dem der Windows 7-Computer mehrmals hintereinander heruntergefahren und neu gestartet wird. Die aufgezeichneten Daten können Sie mit den Tools *Xperf.exe* und *Xperfview.exe* analysieren.

Übung Herunterladen und Benutzen der Windows-Leistungsanalysetools

In dieser Übung laden Sie das Microsoft Windows SDK für Windows 7 und .NET Framework 3.5 SP1 herunter und installieren es, installieren das WPT und zeichnen mit dem Tool *Xperf.exe* eine Ablaufverfolgung auf.

Übung 1 Herunterladen und Installieren des SDKs

In dieser Übung laden Sie das SDK herunter und installieren es. Die Übung enthält einen direkten Link zum Herunterladen einer ISO-Datei mit dem SDK, aber Sie können auch einfach auf der Microsoft-Site nach dem SDK suchen. Gehen Sie folgendermaßen vor:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Legen Sie einen leeren DVD-Rohling in Ihr optisches Laufwerk ein. Schließen Sie das Dialogfeld *Automatische Wiedergabe*.
3. Öffnen Sie Ihren Browser und rufen Sie den Link *http://www.microsoft.com/downloads/details.aspx?familyid=71DEB800-C591-4F97-A900-BEA146E4FAE1* auf.
4. Klicken Sie neben *GRMSDK_EN_DVD.iso* auf die Schaltfläche *Download* (beziehungsweise neben einer der anderen Dateien, wenn Sie eine andere Prozessorarchitektur verwenden).
5. Klicken Sie im Dialogfeld *Dateidownload* auf *Öffnen*. Der Download kann einige Zeit dauern.
6. Klicken Sie auf *Zulassen*, falls ein Sicherheitsdialogfeld des Internet Explorers erscheint.
7. Aktivieren Sie im Dialogfeld *Windows-Brenner für Datenträgerabbilder* das Kontrollkästchen *Datenträger nach dem Brennen überprüfen* und klicken Sie auf *Brennen*.
8. Sobald die DVD gebrannt und überprüft ist, wird sie automatisch ausgeworfen. Schließen Sie *Windows-Brenner für Datenträgerabbilder*. Legen Sie die DVD erneut in das optische Laufwerk ein.
9. Klicken Sie im Dialogfeld *Automatische Wiedergabe* auf *setup.exe ausführen*.
10. Klicken Sie auf *Ja*, falls sich ein Dialogfeld der Benutzerkontensteuerung öffnet.
11. Der Windows SDK Setup Wizard wird gestartet. Klicken Sie auf *Next*.

12. Lesen Sie die Lizenzbedingungen, wählen Sie *I Agree* aus und klicken Sie auf *Next*.
13. Klicken Sie auf *Next*, um die Standardeinstellungen für die Ordner zu übernehmen.
14. Klicken Sie auf *Next*, um die Standardeinstellungen für die Installationsoptionen zu übernehmen.
15. Klicken Sie auf *Next*, um die Installation zu starten.
16. Warten Sie, bis die Installation abgeschlossen ist, und klicken Sie dann auf *Finish*. Lesen Sie die »SDK Release Notes« durch.

Übung 2 Installieren des Windows Performance Toolkits

In dieser Übung installieren Sie die 32-Bit-Version des Windows Performance Toolkit. Falls Ihr Computer unter einem 64-Bit-Betriebssystem läuft, müssen Sie statt *wpt_x86.msi* die Datei *wpt_x64.msi* nehmen. Sie müssen das SDK in Übung 1 installiert haben, bevor Sie diese Übung beginnen.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Öffnen Sie *Computer* und wechseln Sie in den Ordner *C:\Program Files\Microsoft SDKs\Windows\v7.1\Bin*.
3. Klicken Sie doppelt auf die Datei *wpt_x86.msi*. Der Microsoft Windows Performance Toolkit Setup Wizard wird gestartet. Klicken Sie auf *Next*.
4. Stimmen Sie dem Lizenzvertrag zu. Klicken Sie auf *Next*.
5. Klicken Sie auf *Typical* und dann auf *Install*.
6. Klicken Sie auf *Ja*, falls sich ein Dialogfeld der Benutzerkontensteuerung öffnet.
7. Klicken Sie auf *Finish*, sobald das Setup abgeschlossen ist.

Übung 3 Aufzeichnen von Ablaufverfolgungen mit *Xperf.exe*

In dieser Übung verwenden Sie das Trace Capture, Processing, and Command-Line Analysis Tool (*Xperf.exe*), um eine Kernelablaufverfolgung und eine Benutzerablaufverfolgung zu generieren. Sie führen die beiden Ablaufverfolgungen zusammen und verarbeiten die Ergebnisse in einer Textdatei. Sie müssen die Übungen 1 und 2 durchgearbeitet haben, bevor Sie diese Übung beginnen.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
3. Starten Sie die Kernelablaufverfolgung. Für die Kernelsitzung brauchen Sie keinen Namen anzugeben, weil ihr Name eindeutig ist. Die Gruppen *Base* und *Network* sind beim Kernelanbieter aktiviert. Die Ablaufverfolgung wird in einer Datei namens *Kernel.etl* aufgezeichnet. Geben Sie dazu den folgenden Befehl ein:

   ```
   xperf -on Base+Network -f kernel.etl
   ```

4. Starten Sie eine Benutzerablaufverfolgung namens *UserTrace* und aktivieren Sie darin den Anbieter *Microsoft-Windows-Firewall*. Diese Ablaufverfolgung wird in einer Datei namens *User.etl* aufgezeichnet. Geben Sie dazu den folgenden Befehl ein:

   ```
   xperf -start UserTrace -on Microsoft-Windows-Firewall -f user.etl
   ```

5. Beenden Sie die Sitzung *UserTrace*, damit der Benutzermodusanbieter keine Ereignisse mehr für diese Sitzung generiert. Führen Sie dazu den folgenden Befehl aus:

   ```
   xperf -stop UserTrace
   ```

6. Beenden Sie die Kernelsitzung mit dem folgenden Befehl:

   ```
   xperf -stop
   ```

7. Führen Sie Benutzer- und Kernelablaufverfolgung in einer einzigen Ablaufverfolgung namens *Single.etl* zusammen, indem Sie den folgenden Befehl eingeben:

   ```
   xperf -merge user.etl kernel.etl single.etl
   ```

8. Verarbeiten Sie die binäre Ablaufverfolgungsdatei *Single.etl* in eine Textdatei namens *C:\Mytrace.txt*. Führen Sie dazu den folgenden Befehl aus:

   ```
   xperf -i single.etl -o c:\mytrace.txt -a dumper
   ```

Abbildung 13.50 zeigt, wie die Xperf-Befehle in einer Eingabeaufforderung ausgeführt werden. Abbildung 13.51 zeigt einen Ausschnitt aus der erstellten Textdatei. Abbildung 13.52 zeigt, wie die kombinierte Ablaufverfolgung (*Single.eti*) im Performance Analyzer angezeigt wird.

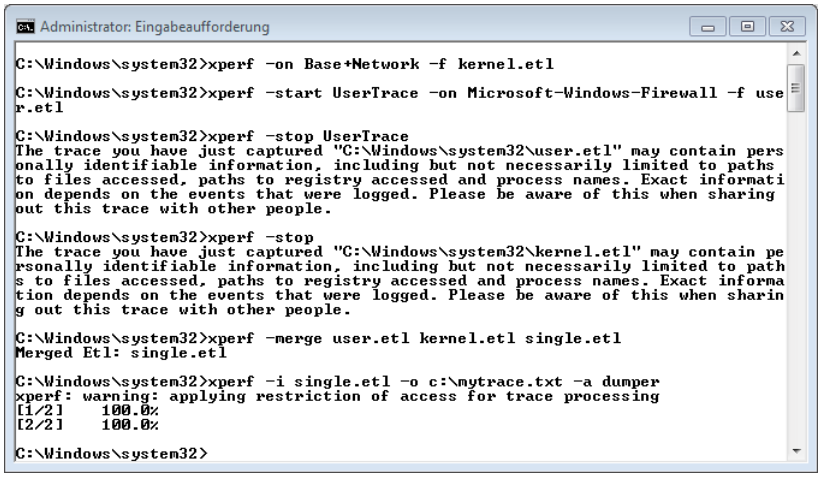

Administrator: Eingabeaufforderung
C:\Windows\system32>xperf -on Base+Network -f kernel.etl
C:\Windows\system32>xperf -start UserTrace -on Microsoft-Windows-Firewall -f user.etl
C:\Windows\system32>xperf -stop UserTrace
The trace you have just captured "C:\Windows\system32\user.etl" may contain personally identifiable information, including but not necessarily limited to paths to files accessed, paths to registry accessed and process names. Exact information depends on the events that were logged. Please be aware of this when sharing out this trace with other people.
C:\Windows\system32>xperf -stop
The trace you have just captured "C:\Windows\system32\kernel.etl" may contain personally identifiable information, including but not necessarily limited to paths to files accessed, paths to registry accessed and process names. Exact information depends on the events that were logged. Please be aware of this when sharing out this trace with other people.
C:\Windows\system32>xperf -merge user.etl kernel.etl single.etl
Merged Etl: single.etl
C:\Windows\system32>xperf -i single.etl -o c:\mytrace.txt -a dumper
xperf: warning: applying restriction of access for trace processing
[1/2] 100.0%
[2/2] 100.0%
C:\Windows\system32>

Abbildung 13.50 Xperf-Befehle zum Aufzeichnen und Zusammenführen von Ablaufverfolgungen

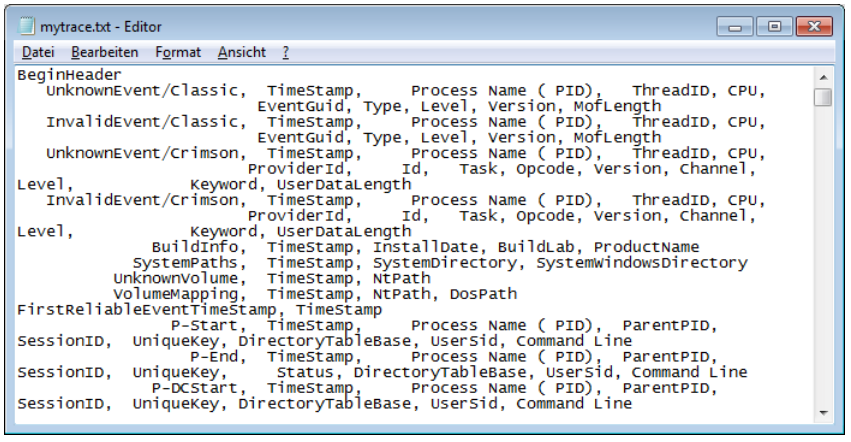

mytrace.txt - Editor
Datei Bearbeiten Format Ansicht ?
BeginHeader
UnknownEvent/Classic, TimeStamp, Process Name (PID), ThreadID, CPU,
EventGuid, Type, Level, Version, MofLength
InvalidEvent/Classic, TimeStamp, Process Name (PID), ThreadID, CPU,
EventGuid, Type, Level, Version, MofLength
UnknownEvent/Crimson, TimeStamp, Process Name (PID), ThreadID, CPU,
ProviderId, Id, Task, Opcode, Version, Channel,
Level, Keyword, UserDataLength
InvalidEvent/Crimson, TimeStamp, Process Name (PID), ThreadID, CPU,
ProviderId, Id, Task, Opcode, Version, Channel,
Level, Keyword, UserDataLength
BuildInfo, TimeStamp, InstallDate, BuildLab, ProductName
SystemPaths, TimeStamp, SystemDirectory, SystemWindowsDirectory
UnknownVolume, TimeStamp, NtPath
VolumeMapping, TimeStamp, NtPath, DosPath
FirstReliableEventTimeStamp, TimeStamp
P-Start, TimeStamp, Process Name (PID), ParentPID,
SessionID, UniqueKey, DirectoryTableBase, UserSid, Command Line
P-End, TimeStamp, Process Name (PID), ParentPID,
SessionID, UniqueKey, Status, DirectoryTableBase, UserSid, Command Line
P-DCStart, TimeStamp, Process Name (PID), ParentPID,
SessionID, UniqueKey, DirectoryTableBase, UserSid, Command Line

Abbildung 13.51 In einer Textdatei aufgezeichnete Ablaufverfolgungsdaten

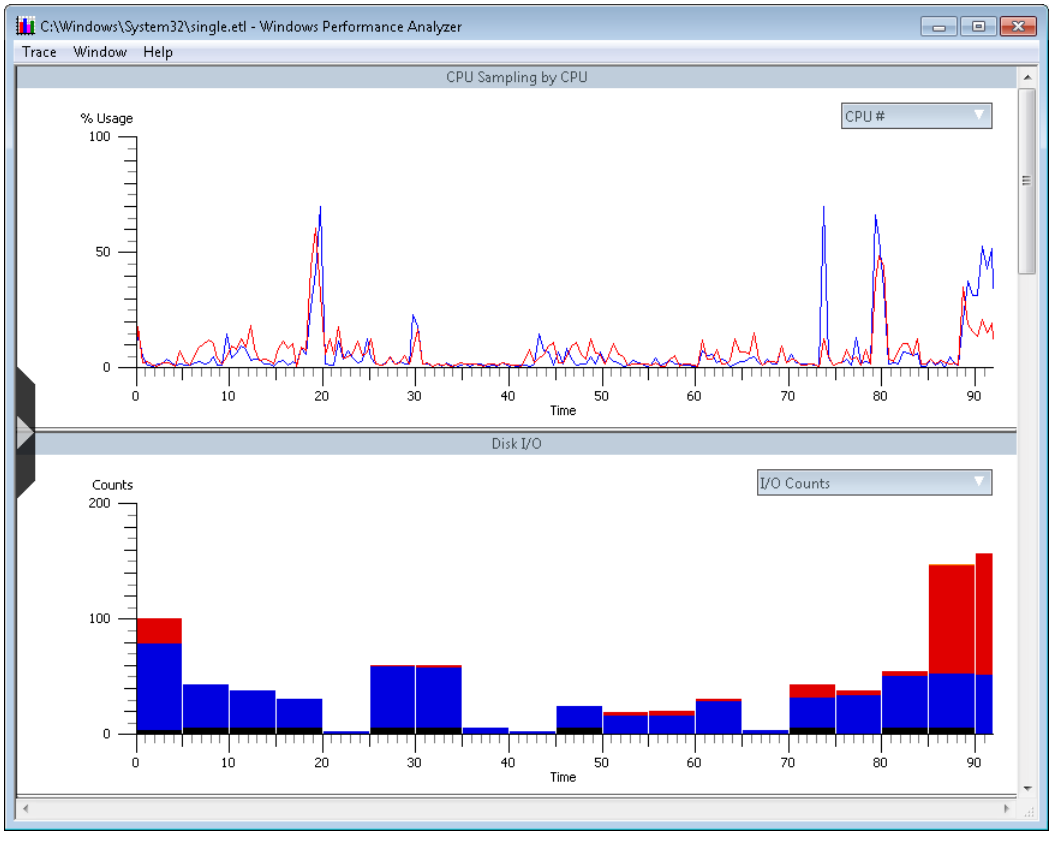


Abbildung 13.52 Aufgezeichnete Ablaufverfolgungsdaten im Performance Analyzer

Zusammenfassung der Lektion

- Sie können WMI-Skripts schreiben, um die Systeminformationen anzupassen, die Sie von einem Computer abrufen, und eigene Tools für die Leistungsmessung zu entwickeln.
- Das Tool *Systemkonfiguration* legt fest, welche Programme beim Systemstart ausgeführt werden, bearbeitet Konfigurationsdateien und ermöglicht Ihnen, Windows-Dienste zu steuern und auf Leistungs- und Problembehandlungswerkzeuge zuzugreifen. In der Konsole *Dienste* verwalten und konfigurieren Sie Dienste; hier stehen mehr Optionen zur Verfügung als auf der Registerkarte *Dienste* des Task-Managers oder der Registerkarte *Dienste* im Tool *Systemkonfiguration*.
- Mit dem Tool *Leistungsoptionen* können Sie visuelle Effekte konfigurieren und festlegen, ob das System für die Leistung von Anwendungen oder Hintergrunddiensten optimiert wird. Sie können darin Einstellungen für Auslagerungsdateien (virtuellen Arbeitsspeicher) und DEP konfigurieren.
- Die Windows-Leistungsanalysetools, die Sie als Teil des Windows 7 SDK herunterladen können, analysieren viele Leistungsprobleme, darunter Anwendungsstartzeiten, Systemstartprobleme, DPCs (Deferred Procedure Call), ISRs (Interrupt Service Request), Probleme mit der Systemreaktionszeit, Auslastung von Anwendungsressourcen und Interruptwellen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Konfigurieren von Leistungseinstellungen«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Welches WMI-Tool benutzen Sie, um sich von der Windows-Verwaltung generierte Ereignisse und Ereignisinformationen anzusehen, beispielsweise Datum und Uhrzeit, Klasse, Herkunft und Beschreibung eines Ereignisses?
   A. WMI CIM Studio
   B. WMI Object Browser
   C. WMI Event Registration Tool
   D. WMI Event Viewer
2. Welches Windows-Leistungsanalysetool zeichnet Benutzer- und Kernelablaufverfolgungen auf und kann sie zusammenführen?
   A. Performance Analyzer
   B. On/Off Transition Trace Capture
   C. Trace Capture, Processing, and Command-Line Analysis
   D. Visual Trace Analysis

3. Welches in Windows 7 enthaltene Tool hilft Ihnen festzustellen, welche Anwendungen für Aktivitäten auf Ihrer Festplatte verantwortlich sind und auf welche Dateien und Ordner zugegriffen wird?
   A. Process Explorer
   B. Ressourcenmonitor
   C. Task-Manager
   D. Windows-Leistungsindex
4. Auf Ihrem Computer sind mehrere rechenintensive Anwendungen sehr langsam gelaufen. Daher haben Sie einen zweiten Prozessor eingebaut. Das beseitigt Ihr Problem aber nicht. Sie untersuchen daher die Prozessorauslastung mit dem Task-Manager und der Leistungsüberwachung. Sie stellen fest, dass mehrere wichtige Prozesse nur den ursprünglichen Prozessor benutzen. Wie stellen Sie sicher, dass diese Prozesse immer auf dem jeweils freien Prozessor ausgeführt werden?
   A. Konfigurieren Sie die Prozesszugehörigkeit auf der Registerkarte *Prozesse* des Task-Managers.
   B. Konfigurieren Sie die Prozesspriorität auf der Registerkarte *Prozesse* des Task-Managers.
   C. Wählen Sie im Tool *Leistungsoptionen* auf der Registerkarte *Erweitert* unter *Optimale Leistung anpassen für* die Option *Programme* aus.
   D. Konfigurieren Sie die Einstellungen für den virtuellen Arbeitsspeicher auf der Registerkarte *Erweitert* des Tools *Leistungsoptionen* neu.
5. Ihr Computer ist als Dual-Boot-System mit Windows Vista Professional und Windows 7 Enterprise eingerichtet. Momentan wird standardmäßig Windows Vista gestartet. Sie möchten Windows 7 als Standardbetriebssystem festlegen und konfigurieren, wie Windows 7 beim Auftreten eines Systemfehlers reagiert. Sie starten den Computer unter Windows 7. Welches Tool benutzen Sie?
   A. Konsole *Dienste*
   B. Leistungsoptionen
   C. Task-Manager
   D. Systemkonfiguration

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Zusammenfassung des Kapitels

- Mithilfe von Windows 7-Tools wie der Leistungsüberwachung, der Zuverlässigkeitsüberwachung, dem Wartungscenter und dem Windows-Zuverlässigkeitsindex können Sie beurteilen, ob Ihr Computer wie gewünscht funktioniert, ob er für die gewünschten Einsatzzwecke aufgerüstet werden sollte und wo Leistungsengpässe auftreten.
- Tools wie der Task-Manager liefern eine Momentaufnahme der aktuellen Auslastung des Computers. Ereignisprotokolle speichern Ereignisse über einen längeren Zeitraum hinweg und können Sie warnen, falls Probleme auftreten. Sammlungssätze zeichnen sowohl aktuelle als auch zurückliegende Leistungsindikatorwerte auf, sodass Sie die aktuelle Leistung des Computers mit einem früheren Zeitpunkt vergleichen können.
- Tools zum Messen und Verbessern der Computerleistung sind WMI-Skripts, das Tool Systemkonfiguration, die Konsole *Dienste*, das Tool Leistungsoptionen und die Windows-Leistungsanalysetools.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Sammlungssatz**
- **Ereignisweiterleitung**
- **Ereignisprotokoll**
- **Ereignisabonnement**
- **Leistungsindikator**

Übungen mit Fallbeispiel

In den folgenden Fallbeispielen wenden Sie an, was Sie über Netzwerkeinstellungen gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Verwenden von Sammlungssätzen und Ereignisweiterleitung

James Seymour ist Administrator für das Produktivnetzwerk von Tailspin Toys. Seit Kurzem beschweren sich die Benutzer über sporadische Leistungsprobleme, wenn sie von ihren Windows 7-Computern aus auf einen Dateiserver zugreifen, der unter Windows Server 2008 R2 läuft. James überprüft die Ressourcenauslastung auf dem Dateiserver mit dem Task-Manager und der Ressourcenübersicht, findet aber nichts, was auf übermäßige Prozessor-, Arbeitsspeicher-, Datenträger- oder Netzwerkauslastung hindeutet. Er muss diese Ressourcen offensichtlich über einen längeren Zeitraum hinweg beobachten, der aktuelle Zustand liefert keine ausreichenden Erkenntnisse. Er muss die Ressourcen dabei sowohl zu Zeiten überwachen, in denen die Leistungsprobleme auftreten, als auch während alles normal läuft. James öffnet auf seinem Windows 7-Computer die Leistungsüberwachung und stellt eine Verbindung zum Dateiserver her.

Beantworten Sie die folgenden Fragen:

1. Wie generiert James Leistungsprotokolle, die ihm bei der Analyse von Datenträger-, Netzwerk-, Prozessor- und Arbeitsspeicherauslastung auf dem Server helfen, und zwar sowohl zu Zeiten, in denen die Leistungsprobleme auftreten, als auch während alles normal läuft?
2. James weiß in etwa, seit wann die Probleme auftreten. Wie kann er feststellen, welche Anwendungen damals installiert oder aktualisiert wurden?
3. Seit Kurzem haben mehrere Benutzer Probleme, Dateien und E-Mail herunterzuladen, weil auf ihrem lokalen Datenträger nicht mehr genug Platz frei ist. James möchte eine vorbeugende Methode entwickeln, Probleme zu erkennen, die durch knappen Festplattenplatz auf den Windows 7-Computern im Netzwerk von Tailspin Toys ausgelöst werden. Auf diese Weise könnte er die Desktopsupporttechniker beauftragen, Festplattenplatz auf solchen Clientcomputern frei zu machen, bevor kritische Limits erreicht werden. Wie überwacht er auf den Clientcomputern Ereignisse, die Warnungen über knappen Festplattenplatz enthalten?

Übung mit Fallbeispiel 2: Problembehandlung für Leistungsprobleme auf einem Clientcomputer

James untersucht Leistungsprobleme auf einem Windows 7-Client bei Wingtip Toys. Das ist normalerweise eine Aufgabe für den Desktopsupport, aber der Computer gehört der Geschäftsführerin, daher muss James die Aufgabe selbst erledigen und schnell eine Lösung finden.

Beantworten Sie folgende Fragen:

1. James führt den Task-Manager aus und stellt fest, dass einer der beiden Prozessoren auf dem Computer stark ausgelastet ist, während der zweite kaum etwas zu tun hat. Er

prüft die Aufzeichnungen und findet heraus, dass vor einiger Zeit jemand aus seinem Team einen zweiten Prozessor eingebaut hat, weil die Geschäftsführerin gehört hatte, dass ein weiterer Prozessor die Leistung ihres Computers verbessern könnte. Wie stellt James sicher, dass die Prozessorressource richtig genutzt wird?

2. James muss schnell die Ereignisse in den Ereignisprotokollen auswerten, die mit der Leistung zu tun haben. Er weiß, dass er Filter und benutzerdefinierte Ansichten erstellen kann, aber das dauert eine Weile und er braucht gleich eine Antwort. Wie kann James schnell auf die entsprechenden Ereignisse zugreifen?
3. Die Geschäftsführerin zieht oft ihre USB-Flashsticks vom Computer ab, ohne sie erst sicher zu entfernen, vor allem, wenn sie in Eile ist. Ihr sind bereits früher Daten auf dem USB-Gerät verloren gegangen. Aber wenn die Geschäftsführerin Daten verliert, ist (natürlich) der technische Support schuld, nicht die Geschäftsführerin. Wie sollte James die Gefahr eines Datenverlusts auf dem USB-Gerät verringern?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Arbeiten mit den Leistungsüberwachungstools

- **Übung 1** Sehen Sie sich die Standardsammlungssätze an, die zur Verfügung stehen, und erstellen Sie versuchsweise eigene. Sammlungssätze sind eine leistungsfähige Methode, um die aktuelle und die frühere Leistung Ihres Computers zu analysieren. Sie werden nur damit vertraut, wenn Sie eine Weile mit ihnen arbeiten.
- **Übung 2** Zu den Aufgaben eines IT-Experten gehört es nicht nur sicherzustellen, dass Computer und Netzwerkgeräte effizient arbeiten, sondern auch, die Ergebnisse der Untersuchungen den Kollegen und dem Management zu berichten. Sie werden danach beurteilt, wie verständlich und relevant die Daten in Ihren Berichten sind. Dies ist auch ein wichtiger Faktor bei Budgetbewilligungen. Lernen Sie, gute Berichte zu generieren.

Verwalten der Ereignisprotokollierung

- Dieses Thema scheint anfangs oft sehr komplex, es wird aber klarer, wenn Sie geübt haben, wie Sie Abonnements konfigurieren und Ereignisse weiterleiten. Sie können dafür erst einmal zwei Computer in Ihrem Testnetzwerk verwenden. Machen Sie sich mit den Abläufen vertraut, bevor Sie diese Aufgaben in einem Produktivnetzwerk ausführen.

Schreiben von WMI-Skripts

- Beispiele für WMI-Skripts finden Sie im Internet und in Fachbüchern. Am einfachsten lernen Sie das Schreiben von Skripts (wie bei jeder Art zu programmieren), wenn Sie die Skripts anderer Leute verstehen und als Grundlage nehmen, bevor Sie eigene Skripts von Grund auf neu schreiben.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

KAPITEL 14

Datensicherung und Wiederherstellung

Die Hardware moderner Computer ist zuverlässig. Es ist ungewöhnlich, wenn ein Computersystem vollständig abstürzt und vollständig wiederhergestellt werden muss. Die meisten Ausfälle werden durch Hardware verursacht. Meist können Sie eine Hardwarekomponente und sogar das gesamte Motherboard ersetzen, ohne dass System- und Benutzerdateien auf Ihrer Festplatte unbrauchbar werden. Dennoch kann es passieren, dass Dateien, Ordner und sogar ganze Volumes verloren gehen, manchmal aufgrund eines Benutzerfehlers, wegen eines Festplattendefekts oder weil ein Virus Sie zwingt, die Festplatte zu löschen.

Datensicherung und Wiederherstellung bleiben daher wichtige Aufgaben für einen IT-Experten. Bei Produktivnetzwerken sind die Abläufe für den Fall einer Serverwiederherstellung normalerweise gut dokumentiert, und Server werden oft in Failoverkonfigurationen zusammengefasst. Falls die Benutzerdaten nicht zentral gespeichert und gesichert werden, müssen regelmäßige Datensicherungen wichtiger Dateien auf den Clientcomputern geplant werden. Das sollte ohne Benutzereingriffe laufen, am besten nachts, wenn die Datensicherung Benutzer nicht bei der Arbeit stört.

In diesem Kapitel erfahren Sie, wie Sie sowohl Dateien als auch Ordner und Systemabbilder sichern und Datensicherungen so planen, dass sie zur angegebenen Zeit automatisch ausgeführt werden. Sie lernen, wie Sie eine wichtige Datei schnell wiederherstellen, wenn ein Benutzer sie verloren oder überschrieben hat. Und Sie erfahren, wie Sie das Systemabbild für ein gesamtes Systemvolume erstellen und wiederherstellen.

In diesem Kapitel abgedeckte Prüfungsziele:

- Konfigurieren der Datensicherung
- Konfigurieren von Systemwiederherstellungsoptionen
- Konfigurieren von Dateiwiederherstellungsoptionen

Lektionen in diesem Kapitel:

- Lektion 1: Datensicherung 735
- Lektion 2: Systemwiederherstellung 751
- Lektion 3: Wiederherstellen von Dateien und Ordnern 768

Bevor Sie beginnen

Um die Übungen in diesem Kapitel durchzuarbeiten, müssen Sie folgende Vorbereitungen getroffen haben:

- Sie haben Windows 7 auf einem eigenständigen Client-PC installiert, wie in Kapitel 1, »Installieren, Migrieren oder Aktualisieren auf Windows 7«, beschrieben.
- Sie haben eine zweite Festplatte auf diesem Computer bereitgestellt. Das kann eine interne Festplatte oder eine externe USB-Festplatte (Universal Serial Bus) sein. Sie muss mit dem Dateisystem NTFS formatiert sein. Auf der Festplatte müssen mindestens 20 GByte Platz frei sein.

Praxistipp

Ian McLean

Viele Leute unterscheiden nicht zwischen den Begriffen *Datensicherung* (backup) und *Kopie* (copy). Wenn ich heute Abend meine Arbeit an diesem Kapitel beende, kopiere ich sie auf ein USB-Flashlaufwerk, das ich getrennt von meinem Computer aufbewahre. Sollte mein Computer einen Defekt haben oder gestohlen werden, ist zumindest nicht meine gesamte Arbeit verloren. Einmal wöchentlich werden alle meine Benutzerdateien automatisch auf eine externe Festplatte gesichert, die ich bei Bedarf an einen anderen Computer anschließen kann. In beiden Fällen schütze ich meine Daten. Wo liegt also der Unterschied?

Wenn eine Datei gesichert wird, wird ihr Archivattribut gesetzt. Sofern sich die Datei nicht verändert hat, wird sie bei einer geplanten Datensicherung nicht erneut gesichert. Falls mehrere Benutzer mit demselben Computer arbeiten, sichert eine Datensicherung die Dateien aller Benutzer. Ein Standardbenutzer kann nur seine eigenen Dateien kopieren.

Beim Kopieren von Dateien ist es nicht möglich, Registrierungseinstellungen oder andere Systemeinstellungen zu sichern. Beim Kopieren von Dateien kann kein vollständiges Abbild eines Computers oder Systemvolumes erstellt werden. Datensicherungen sind komprimiert und brauchen weniger Festplattenplatz als Kopien. Die Komprimierung während der Datensicherung und die Dekomprimierung während der Wiederherstellung werden automatisch durchgeführt, für den Benutzer sind sie unsichtbar. Sie können den Assistenten *Dateien wiederherstellen* nicht einsetzen, um Dateien wiederherzustellen, die Sie kopiert haben.

Kopien werden nicht als Vorgängerversionen markiert. Sie können nicht das Feature *Vorgängerversionen wiederherstellen* nutzen, um sie wiederherzustellen. Sie können Dateien von beliebigen Medien auf andere Medien kopieren. Sie können keine Dateien sichern, die auf FAT-Medien gespeichert sind. Sie können Dateien nur auf einer Festplatte (intern, extern oder Netzlaufwerk), auf optischen Medien, auf einer virtuellen Festplatte (Virtual Hard Disk, VHD) oder auf einem anderen Computer sichern.

Und schließlich können Sie Dateien kopieren, die Sie verschlüsselt haben. Sie können verschlüsselte Dateien nicht sichern. Wie lautet also eine vernünftige Empfehlung, wenn es um Kopien geht? Sollten Sie als IT-Experte die Benutzer, für die Sie Support leisten, ermutigen, ihre Dateien zu kopieren? An sich leuchtet das Konzept ein, dass die Benutzer sich bewusst sein sollten, dass ihre Daten geschützt werden müssen. Aber die Presse liebt Geschichten über verlorene USB-Flashlaufwerke, die vertrauliche Daten enthalten.

(Optische Datenträger gehen genauso leicht verloren, aber aus irgendeinem Grund begeistern sich Journalisten vor allem für Geschichten, in denen USB-Sticks vorkommen.) Stellen Sie also entweder sicher, dass alle Benutzer ihre Dateien verschlüsseln, oder verbieten Sie ihnen, Kopien zu machen.

Für was auch immer Sie sich entscheiden: Beliebt machen Sie sich damit nicht.

Lektion 1: Datensicherung

In dieser Lektion erfahren Sie, wie Sie in der Konsole *Sichern und Wiederherstellen* eine Datei- und Ordnersicherung planen und einen Systemreparaturdatenträger erstellen. Sie lernen, wie Sie einen Zeitplan für die Datei- und Ordnersicherung festlegen und auswählen, welche Dateien und Ordner dabei gesichert werden. Sie können in der Konsole *Sichern und Wiederherstellen* auch ein Abbild eines ganzen Volumes erstellen. Wenn Sie solche Systemabbildsicherungen allerdings nach einem Zeitplan ausführen wollen, müssen Sie eine Batchdatei schreiben, die Befehlszeilenanweisungen enthält. Schließlich erfahren Sie noch, wie Sie eine Systemabbildsicherung in einer Eingabeaufforderung mit erhöhten Rechten auslösen.

Ein *Systemabbild* (system image) ist eine Kopie aller Dateien und Ordner auf dem Systemdatenträger (und anderen angegebenen Festplatten) eines Computers. Mithilfe einer Systemabbildsicherung können Sie den Computer genau in dem Zustand wiederherstellen, in dem er war, als die Systemabbildsicherung erstellt wurde.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Festlegen eines Zeitplans für eine Datei- und Ordnersicherung in der Konsole *Sichern und Wiederherstellen* und Durchführen einer Systemabbildsicherung
- Erstellen eines Systemreparaturdatenträgers
- Beschreiben der Dateistruktur einer Datensicherung und eines Sicherungssatzes
- Erstellen einer Systemabbildsicherung in einer Eingabeaufforderung mit erhöhten Rechten

Veranschlagte Zeit für diese Lektion: 35 Minuten

Planen von Datensicherungen in der Konsole *Sichern und Wiederherstellen*

Die Windows 7-Datensicherung nutzt Schattenkopien, um einen Snapshot Ihrer Dateien anzufertigen. Auf diese Weise kann die Datensicherung die Dateien vollständig sichern, selbst wenn sie gerade geöffnet sind. Datensicherungen werden in der Konsole *Sichern und Wiederherstellen* konfiguriert und geplant. Sie öffnen diese Konsole in der Systemsteuerung unter *System und Sicherheit*. Wenn Sie die Konsole *Sichern und Wiederherstellen* zum ersten Mal öffnen (wenn also noch keine geplanten Datensicherungen auf Ihrem Computer konfiguriert sind), sieht sie ähnlich aus wie in Abbildung 14.1.

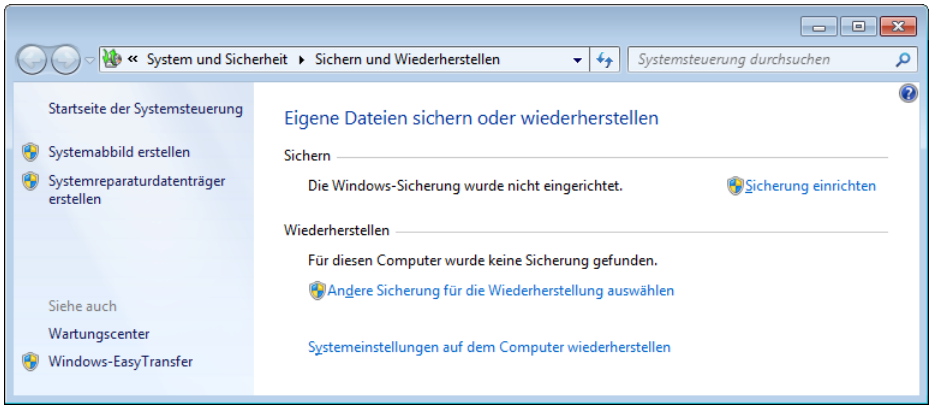


Abbildung 14.1 Die Konsole *Sichern und Wiederherstellen*, wenn noch keine Datensicherungen konfiguriert sind

In diesem Fall besteht eine Ihrer ersten Aufgaben darin, regelmäßige Datensicherungen zu konfigurieren. Klicken Sie dazu auf *Sicherung einrichten*. Sie werden nun aufgefordert, ein Ziel für die Datensicherung anzugeben (Abbildung 14.2).

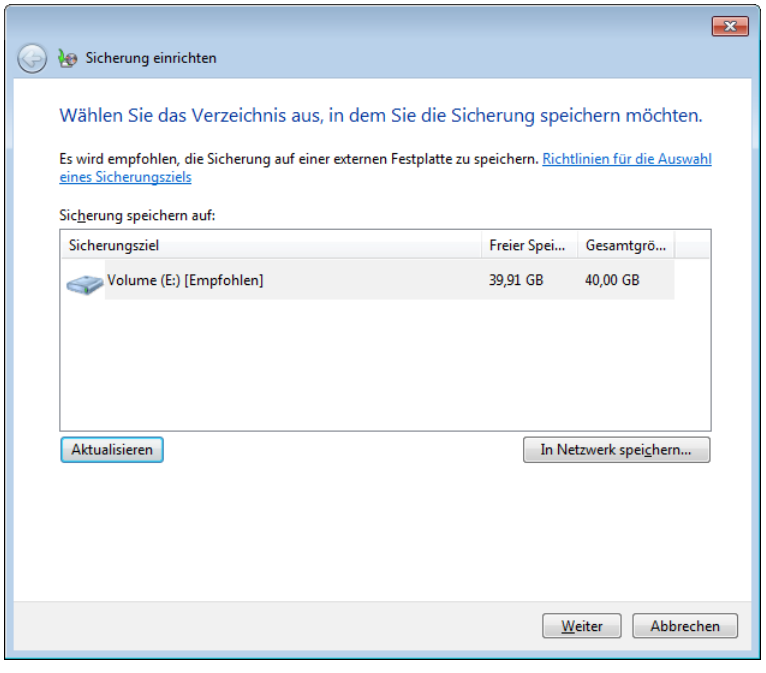


Abbildung 14.2 Auswählen eines Datensicherungsziels

Es stehen folgende Typen von Datensicherungszielen zur Auswahl:

- **Zweites internes Festplattenlaufwerk** Festplattenlaufwerke sind sicher (besonders wenn sie mit NTFS formatiert sind), vergleichsweise billig und im Allgemeinen ständig verfügbar. Sie können das Laufwerk in einem anderen Computer installieren, wenn Sie gesicherte Daten auf diesem Computer wiederherstellen wollen. Ein zweites Festplat-

tenlaufwerk in einen Computer einzubauen und es dann in einen anderen Computer einzubauen, ist bei Weitem nicht so einfach wie ein externes Gerät anzustecken. Wenn Ihr Computer zwei interne Festplattenlaufwerke hat und Sie ein Dual-Boot-System eingerichtet haben, bei dem auf jeder Festplatte jeweils ein Betriebssystem läuft, können Sie die jeweils andere Festplatte nicht als Datensicherungsziel verwenden.



Warnung Speichern von Datensicherungen auf einem Datenträgervolume

Speichern Sie Ihre Datensicherungen nicht auf einer separaten Partition auf der einzigen Festplatte Ihres Computers. Wenn das Festplattenlaufwerk aufgrund eines Hardwaredefekts ausfällt oder wegen eines Virenangriffs gelöscht werden muss, verlieren Sie auch Ihre Datensicherung.

- **Externes Festplattenlaufwerk** Externe Festplattenlaufwerke sind in der Anschaffung teurer als interne Festplattenlaufwerke, aber Sie müssen bei einer internen Festplatte auch die Kosten für den Einbau berücksichtigen. Externe Festplattenlaufwerke können entfernt und an einem sicheren Ort aufbewahrt werden. Sie sind aber meist langsamer als interne Festplattenlaufwerke und oft sind sie nicht so zuverlässig, vor allem weil sie oft standardmäßig mit FAT formatiert sind statt mit NTFS. Sie können ein externes Festplattenlaufwerk nicht für eine Systemabbildsicherung einsetzen, wenn Sie sein Dateisystem nicht vorher in NTFS konvertieren. Weil es einfach zu entfernen ist, ist die Gefahr größer, dass ein externes Festplattenlaufwerk nicht verfügbar ist, wenn eine geplante Datensicherung ansteht.
- **DVD** Optische Datenträger sind billig und können an einem sicheren Ort aufbewahrt werden. Sie können für die Datensicherung sowohl CDs als auch DVDs verwenden, aber in der Praxis bräuchten Sie für eine typische Datensicherung eine Unmenge CDs. Wahrscheinlich würden Sie auch eine ganze Reihe DVDs brauchen. Geplante Systemabbildsicherungen können Sie nicht auf DVDs speichern. DVDs gehen im Lauf der Zeit manchmal kaputt, aber meist erst nach einigen Jahren.
- **USB-Flashlaufwerke** Flashspeicher ist in den letzten 2 bis 3 Jahren deutlich billiger geworden, und die Flashlaufwerkgeräte haben immer größere Kapazität. Trotzdem bieten sie normalerweise deutlich weniger Speicher als Festplattenlaufwerke. Wenn Sie Kopien älterer Datensicherungen behalten wollen, füllen Sie sich allzu schnell. Sie können in einem Flashspeichergerät keine Systemabbildsicherungen speichern. Ein Flashlaufwerk muss mehr als 1 GByte Platz bieten, wenn Sie eine Datensicherung darauf speichern wollen. Flashlaufwerke können problemlos an einem weit entfernten Ort aufbewahrt werden, da sie klein und leicht sind. Allerdings gehen sie auch leicht verloren.
- **Netzwerkspeicherort** Wenn der Festplattenplatz auf Ihrem Computer knapp ist, können Sie für die Datensicherung auch einen Netzwerkspeicherort auf einem anderen Computer oder Netzwerkspeicher verwenden. Beachten Sie, dass dies eine andere Konstellation ist als in einer Produktivumgebung, wo die Dokumentbibliotheken der Benutzer auf einem Dateiserver gespeichert sind und ein Administrator den Dateiserver sichert. Sie können Ihre Datensicherungen nur mit Windows 7 Professional, Windows 7 Ultimate und Windows 7 Enterprise in einem Netzwerkspeicherort speichern. Außerdem brauchen Sie entsprechende Anmeldeinformationen, damit die Windows-Sicherung auf das Netzwerk zugreifen kann.

- **VHD** In Windows 7 können Sie eine VHD als Ziel einer Datensicherung verwenden. Die VHD-Datei sollte sich aber nicht auf der physischen Festplatte befinden, die Sie sichern, sonst geht bei einem Defekt der Festplatte auch Ihre Datensicherung verloren. Sie können auch die Systemabbildsicherung eines gesamten Volumes in eine VHD schreiben. Unter Windows 7 Ultimate und Enterprise Edition können Sie eine VHD mit dem Tool BCDEdit startfähig machen, sodass Sie den Computer von einem gesicherten Systemabbild starten können.

Wählen Sie das gewünschte Datensicherungsmedium aus und klicken Sie auf *Weiter*. Sie haben nun die Wahl, Windows auswählen zu lassen, welche Dateien und Ordner gesichert werden, oder die Dateien selbst auszuwählen. Wenn Sie Windows die Entscheidung überlassen, umfasst Ihre Datensicherung Datendateien, die lokal in Bibliotheken, auf dem Desktop und in Windows-Standardordnern gespeichert sind, und zwar von allen Benutzern, die Konten auf dem Computer haben. Windows-Standardordner sind *AppData*, *Contacts*, *Desktop*, *Downloads*, *Favorites*, *Links*, *Saved Games* und *Searches*. Sofern das Laufwerk, auf dem Sie Ihre Datensicherung speichern, mit NTFS formatiert und genug Platz darauf frei ist, wird auch ein Systemabbild Ihrer Programme, Ihres Betriebssystems und aller Treiber und Registrierungseinstellungen in die Datensicherung integriert. In der Konsole *Sichern und Wiederherstellen* können Sie aber keine regelmäßige Systemabbildsicherung planen.

Wenn Sie selbst auswählen wollen, welche Dateien gesichert werden, können Sie die lokalen Dateien und Ordner markieren, außer den *Program Files* (Anwendungen), Dateien von Festplatten, die mit dem Dateisystem FAT formatiert sind, Dateien im Papierkorb und temporären Dateien auf Laufwerken, die kleiner sind als 1 GByte. Sie können auch festlegen, ob Ihre Datensicherung ein Systemabbild der Laufwerke umfasst, die ein Betriebssystem enthalten (sofern Ihr Datensicherungsziel diese Möglichkeit unterstützt).

Sie können bei Bedarf *Zusätzliche Speicherorte* auswählen. Damit werden Elemente wie Favoriten, gespeicherte Spielstände, Suchoperationen, Desktopdaten und Links gesichert. Außerdem haben Sie die Möglichkeit, die Bibliothek *Dokumente* zu sichern. Wenn Sie sicherstellen wollen, dass ein bestimmtes Verzeichnis gesichert wird, können Sie es direkt auswählen oder (wenn Sie Windows auswählen lassen, welche Ordner gesichert werden) das Verzeichnis zur Dokumentbibliothek hinzufügen. Wenn Sie Windows die Auswahl überlassen, welche Ordner gesichert werden, sichert es die Dokumentbibliothek immer.



Prüfungstipp

Denken Sie daran, dass Bibliotheken virtuelle Ordner sind. Sie können Ordner zu Bibliotheken hinzufügen, Sie können Ordner aber nicht in Bibliotheken verschieben.

Sobald Sie ausgewählt haben, was Sie sichern wollen (oder Windows auswählen lassen), werden Sie aufgefordert, die Einstellungen für Ihre Datensicherung zu überprüfen. In der Standardeinstellung werden Datensicherungen jeden Sonntag um 19:00 ausgeführt. Wenn das schlecht passt, können Sie auf *Zeitplan ändern* klicken. Sind Sie mit allen Einstellungen einverstanden, können Sie auf *Einstellungen speichern und Sicherung ausführen* klicken. Die Datensicherung wird dann sofort ausgeführt (und erneut zum geplanten Zeitpunkt). Abbildung 14.3 zeigt die Konsole *Sichern und Wiederherstellen*, nachdem Sie eine geplante Datensicherung konfiguriert haben.

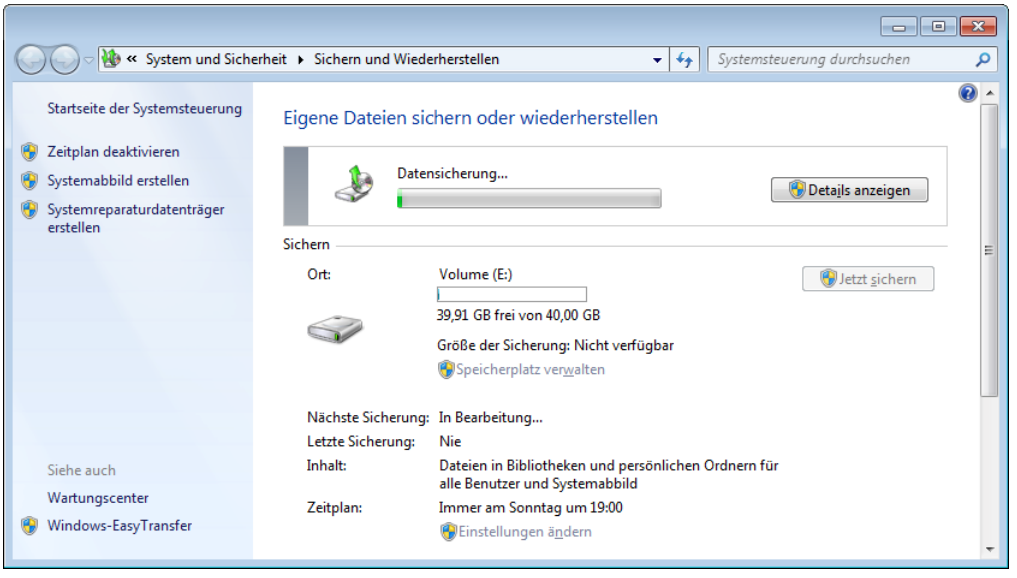


Abbildung 14.3 Die Konsole *Sichern und Wiederherstellen* zeigt, dass eine Datensicherung gestartet wurde

Die Konsole *Sichern und Wiederherstellen* unterstützt zwei Arten von Datensicherung:

- **Systemabbild** Die Systemabbildsicherung sichert ein ganzes Volume in einer *.vhd*-Abbilddatei (die komprimiert wurde, sodass leere Bereiche keinen Platz verbrauchen). Bei dieser Art Datensicherung können Sie einen Computer inklusive aller laufenden Anwendungen schnell wiederherstellen. Wenn Sie allerdings von diesem Abbild starten, was in den Windows 7-Editionen Enterprise und Ultimate möglich ist, müssen Sie sicherstellen, dass das Abbild auf dem neusten Stand gehalten wird. Andernfalls starten Sie mit einem unsicheren Abbild, weil Updates, die Sicherheitslücken schließen, nicht installiert sind. Kapitel 2, »Konfigurieren von Systemabbildern«, beschäftigt sich mit diesem Problem.
- **Dateien und Ordner** Sie können Dateien und Dokumente in komprimierten Dateien (*.zip*) speichern. Dateisicherungen sind standardmäßig inkrementell. Außerdem werden bei Dateisicherungen keine Systemdateien, Programmdateien, mit EFS (Encrypting File System) verschlüsselte Dateien, temporäre Dateien, Dateien im Papierkorb oder Benutzerprofileinstellungen gesichert. Dateisicherungen können auf lokalen Medien oder in einem freigegebenen Ordner im Netzwerk gespeichert werden.



Hinweis **Bereitstellen eines Systemabbilds in Microsoft Windows Virtual PC**

Sie können ein Systemabbild, das von der Systemabbildsicherung erstellt wurde, auch in Windows Virtual PC bereitstellen. Windows Virtual PC steht zur Verfügung, wenn Sie den Windows XP-Modus installieren.



Weitere Informationen Virtual PC und Windows XP-Modus

Weitere Informationen über Virtual PC und den Windows XP-Modus finden Sie unter *http://www.microsoft.com/windows/virtual-pc/*. Klicken Sie dort auf die gewünschten Links.



Prüfungstipp

Denken Sie daran, dass das Tool *Sichern und Wiederherstellen* in Windows 7 Systemabbildsicherungen im VHD-Format schreibt. In den Windows 7-Editionen Enterprise und Ultimate können Sie eine solche Datensicherung mithilfe des Tools Diskpart und der Konsole *Datenträgerverwaltung* im Dateisystem bereitstellen und die VHD dann mit dem Tool BCDEdit startfähig machen. Das Tool *Sichern und Wiederherstellen* schreibt Systemabbildsicherungen in keinen anderen Dateiformaten wie etwa ISO, WIM oder BAK.

Schnelltest

- Alle Clientcomputer in Ihrem Produktivnetzwerk laufen unter Windows 7 Enterprise. Alle haben eine einzige interne Festplatte. Sie möchten keine externe Festplatte für jeden Clientcomputer bereitstellen. Es sollen regelmäßige Systemabbildsicherungen durchgeführt werden. Welche Art von Datensicherungsziel verwenden Sie?

Antwort zum Schnelltest

- In diesem Fall schreiben Sie die Datensicherung in eine Netzwerkfreigabe, die sich entweder auf einem Netzwerkspeichersystem oder auf einem Dateiserver befindet.

Das Tool *Sichern und Wiederherstellen* in Windows 7 bietet die Möglichkeit, Datendateien auf CD, DVD, Festplatte (auch VHD-Dateien) oder in einen Netzwerkspeicherort zu schreiben. Sie können mit *Sichern und Wiederherstellen* eine Systemabbildsicherung auf ein internes Festplattenlaufwerk, ein externes Festplattenlaufwerk (sofern es mit NTFS formatiert ist) und einen Netzwerkspeicherort schreiben. Sie können mit *Sichern und Wiederherstellen* aber keine Systemabbildsicherung auf ein USB-Flashlaufwerk, auf eine DVD oder ein Bandlaufwerk schreiben.

Denken Sie daran, dass es nur mit Windows 7 Professional, Windows 7 Ultimate und Windows 7 Enterprise möglich ist, eine Datensicherung auf einen Netzwerkspeicherort zu schreiben. Und vergessen Sie nicht, dass Bandlaufwerke vom Tool *Sichern und Wiederherstellen* nicht unterstützt werden.



Hinweis BitLocker

Sie können kein Datensicherungsziel auswählen, bei dem BitLocker aktiviert ist.

Datei- und Ordnersicherung

In der grafischen Benutzeroberfläche (Graphical User Interface, GUI) der Konsole *Sichern und Wiederherstellen* können Sie Datensicherungen manuell auslösen und automatische Datensicherungen planen. Sie müssen automatische Datensicherungen auf allen Clientcomputern planen, die wichtige Daten enthalten. Sobald Sie die automatische Dateisicherung in der Konsole *Sichern und Wiederherstellen* konfiguriert haben, sichert Windows 7 regelmäßig

Ihre Dateien. Wenn das erste Mal eine Datensicherung durchgeführt wird, wird sie als vollständige Datensicherung ausgeführt, sie speichert also alle wichtigen Benutzerdokumente. Nachfolgende Datensicherungen sind dagegen inkrementell, es werden also nur geänderte Dateien gesichert. Wenn kein Platz mehr auf dem Zieldatenträger frei ist, werden ältere Datensicherungen gelöscht.

Wenn Sie beispielsweise eine Datensicherung planen, die jede Nacht ausgeführt wird, und eine Datei jeden Tag ändern, wird in jedem Sicherungsdateienordner eines Tages eine Kopie dieser Datei gespeichert. Weil Windows 7 mehrere Versionen derselben Datei speichert, haben Benutzer die Möglichkeit, zwischen mehreren alten Exemplaren einer Datei auszuwählen, wenn sie das Tool *Vorgängerversionen* verwenden (mehr dazu in Lektion 3, »Wiederherstellen von Dateien und Ordnern«). Wenn Sie Dateien wiederherstellen, brauchen Sie nur eine einzige Datensicherung, weil Windows 7 automatisch die neuste Version jeder Datei sucht. Windows 7 verwendet Schattenkopien (beschrieben in Lektion 3), um die letzte gespeicherte Version einer Datei zu sichern. Wenn daher eine Datei geöffnet ist, während die Datensicherung läuft, wird diese Datei gesichert. Änderungen, die der Benutzer vorgenommen hat, seit die Datei zuletzt gesichert wurde, werden dabei allerdings nicht gespeichert.

Sie brauchen Administratoranmeldeinformationen, um geplante Datensicherungen zu konfigurieren oder von Hand eine Datensicherung auszulösen. Zum Wiederherstellen von Dateien werden dagegen keine Administratorprivilegien benötigt, sofern ein Benutzer nicht die Datei eines anderen wiederherstellen will.

Wenn Sie eine Dateisicherung in einen freigegebenen Netzwerkordner schreiben, müssen die Anmeldeinformationen, unter denen die Datensicherung läuft, die Freigabe- und NTFS-Berechtigung *Vollzugriff* für den Zielordner haben (im Windows 7 Setup-Assistenten als *Mitbesitzer*-Berechtigungen bezeichnet). Um die Sicherheit nicht zu gefährden, sollten Sie dafür ein Benutzerkonto einrichten, das nur von der Datensicherungsanwendung verwendet wird, und die Freigabe- und NTFS-Berechtigungen so konfigurieren, dass sie nur diesem Datensicherungskonto Zugriff gewähren. Das Datensicherungskonto braucht auf dem Computer, auf dem die Datensicherung gespeichert wird, administrative Privilegien, aber diese Berechtigungen werden nur für die Freigabe und Ordner des Zielcomputers benötigt.

Ordnerstruktur bei der Datei- und Ordnersicherung

Wenn ein Benutzer eine Datensicherung auf einer externen Festplatte durchführt, legt Windows 7 im Stammverzeichnis der Festplatte automatisch einen Ordner an, dessen Name dem Computernamen entspricht. In diesem Ordner werden die Datensicherungen im Format *Backup Set <Jahr-Monat-Tag> <Uhrzeit>* gespeichert. Wenn also der Name Ihres Computers *Canberra* lautet, Sie die Datensicherung in *H:* speichern und eine Datensicherung am 14. Dezember 2009 um 17:31:54 durchführen, liegt diese Datensicherung in *H:\Canberra\Backup Set 2009-12-14 173154* (Abbildung 14.4).

Die Ordnerstruktur wird erstellt, wenn Sie zum ersten Mal eine Datensicherung ausführen. Der Name des *Backup Set*-Ordners wird aber niemals aktualisiert, daher sind die Dateien neuer, als das Datum im Ordnernamen vermuten lässt. Ein neuer *Backup Set*-Ordner wird nur erstellt, wenn Sie eine vollständige Datensicherung durchführen.

Innerhalb jedes *Backup Set*-Ordners legt die Datensicherung mehrere Ordner an, deren Namen sich aus dem Datum ableiten, an dem die inkrementelle Datensicherung durchgeführt wurde. Zusätzlich legt die Datensicherung im *Backup Set*-Ordner einen Ordner namens *Catalogs* an. Abbildung 14.5 zeigt die Ordnerstruktur für Datensicherungen des Computers

Canberra. Die Datei- und Ordnersicherung wird im Ordner *Canberra* gespeichert. In diesem Fall wurde keine Systemabbildsicherung durchgeführt, weil dies erst weiter unten in dieser Lektion behandelt wird; dabei verwenden Sie eine Eingabeaufforderung mit erhöhten Rechten. Würde in diesem Beispiel allerdings eine Systemabbildsicherung durchgeführt, würde sie im Ordner *WindowsImageBackup* auf dem Laufwerk *H:* gespeichert. Die Dateiberechtigungen sind bei allen Ordnern und Dateien auf Administratoren, die Vollzugriff haben, und auf den Benutzer beschränkt, der die Datensicherung konfiguriert hat; dieser Benutzer hat standardmäßig nur Leseberechtigung.

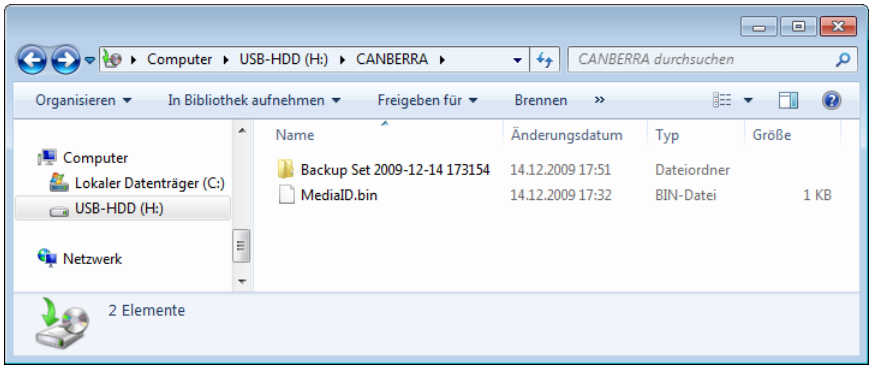


Abbildung 14.4 Sicherungssatz

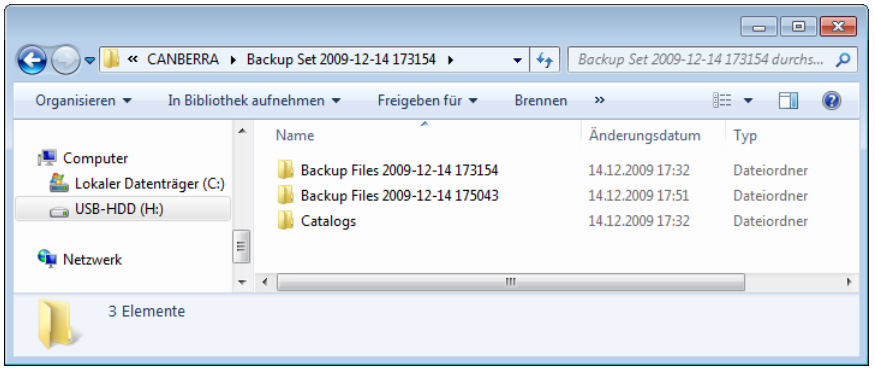


Abbildung 14.5 Ordnerstruktur der Datensicherung

In jedem Datensicherungsordner liegt eine Reihe komprimierter Dateien (*.zip*) mit dem Namen *Backup files <xxx>.zip*, wobei *<xxx>* eine Zahl ist, die bei jeder Datei erhöht wird, sodass der Dateiname eindeutig ist. Zum Beispiel kann ein Datensicherungsordner folgende Dateien enthalten:

- *Backup files 1.zip*
- *Backup files 2.zip*
- *Backup files 3.zip*

Dies sind standardmäßig komprimierte Dateien, die Sie mit den integrierten Dekomprimierungsfunktionen von Windows 7 oder den Tools anderer Hersteller öffnen können. Weil Windows 7 komprimierte Dateien durchsuchen kann, können Sie eine bestimmte Datei in

einer Datensicherung finden, indem Sie die Datensicherungsordner durchsuchen und die Datei dann aus dem komprimierten Ordner extrahieren. Sie brauchen dazu nicht die Konsole *Sichern und Wiederherstellen* zu öffnen. Sie können Dateien wiederherstellen, die in Windows 7 gesichert wurden, selbst wenn Sie Ihren Computer unter einem anderen Betriebssystem starten.

Der Ordner *Catalogs* enthält eine Datei namens *GlobalCatalog.wbcat*. Sie enthält einen Index der einzelnen Dateien, die gesichert wurden, sowie der komprimierten Datei, in der die Datensicherung enthalten ist. Windows 7 ist mithilfe dieser Informationen in der Lage, eine Datei schnell zu finden, wenn sie wiederhergestellt werden soll. Der Ordner *Catalogs* enthält auch eine Liste mit den Dateiberechtigungen aller gesicherten Dateien. Daher sind die Berechtigungen unverändert, wenn Sie Dateien wiederherstellen, zumindest sofern Sie dazu die Konsole *Sichern und Wiederherstellen* verwenden. Stellen Sie eine Datei dagegen direkt aus dem komprimierten Ordner her, erbt die Datei die Berechtigungen des übergeordneten Ordners, in dem sie wiederhergestellt wird; sie behält also nicht die Dateiberechtigungen der ursprünglichen Datei.

Durchführen von Systemabbildsicherungen

Systemabbildsicherungen sichern Ihr Systemvolume Block für Block in einer *.vhd*-Datei, die in lokalen Speicher geschrieben wird, etwa auf einer zweiten Festplatte. Sie können eine *.vhd*-Datei sogar dann auf einer zweiten Festplatte speichern, wenn diese Festplatte ein anderes Betriebssystem enthält. Nachfolgende Datensicherungen auf dasselbe Medium führen automatisch eine inkrementelle Sicherung durch. Nur die Teile der Festplatte, die sich geändert haben, werden in die vorhandene Systemabbildsicherung kopiert. Es wird nur eine einzige Version der Systemabbildsicherung gespeichert.

Die Konsole *Sichern und Wiederherstellen* stellt keine grafische Oberfläche zur Verfügung, um Systemabbildsicherungen zu planen. Eine Systemabbildsicherung müssen Sie von Hand in der Konsole *Sichern und Wiederherstellen* ausführen. Das sollten Sie immer tun, nachdem Sie größere Änderungen an der Konfiguration des Computers vorgenommen haben. Bei einem Punkt müssen Sie allerdings vorsichtig sein: Wenn Sie eine Systemabbildsicherung wiederherstellen und davon starten oder die VHD startfähig machen, um Failoverschutz zu gewährleisten, weist Ihr Computer unter Umständen Sicherheitslücken auf, sofern das Systemabbild nicht mit Sicherheitsupdates aktualisiert wurde.

Auch wenn es nicht möglich ist, in der Konsole *Sichern und Wiederherstellen* einen Zeitplan für Systemabbildsicherungen zu konfigurieren, können Sie für diesen Zweck das Befehlszeilenprogramm Wbadmin verwenden. Beispielsweise lösen Sie eine Systemabbildsicherung des Laufwerks *C:* auf Laufwerk *H:* aus, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten den folgenden Befehl ausführen:

```
wbadmin start backup -backuptarget:h: -include:c: -quiet
```

Abbildung 14.6 zeigt einen Ausschnitt aus der Ausgabe dieses Befehls. Beachten Sie, dass das Laufwerk *H:* mit dem Dateisystem NTFS formatiert sein muss, wenn es für eine Systemabbildsicherung benutzt werden soll. Wenn das Volume, das Sie sichern (in diesem Fall Laufwerk *C:*), eine VHD enthält und diese VHD im Dateisystem bereitgestellt wurde, werden die Dateien aus dieser VHD nicht gesichert. Wenn Sie eine Systemabbildsicherung zum ersten Mal ausführen, sichert sie alle Blöcke des Systemvolumes. Bei den nachfolgenden Datensicherungen werden nur die geänderten Abschnitte aktualisiert.

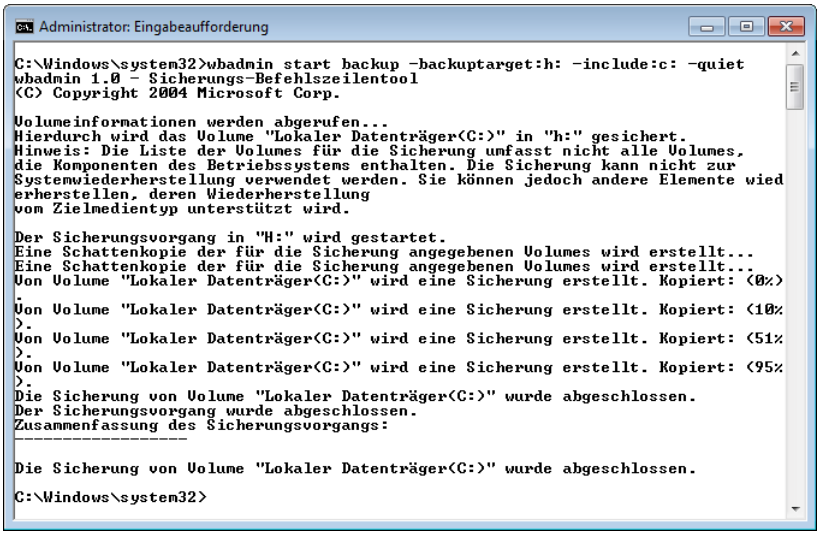

Administrator: Eingabeaufforderung
C:\Windows\system32>wbadmin start backup -backuptarget:h: -include:c: -quiet
wbadmin 1.0 - Sicherungs-Befehlszeilentool
(C) Copyright 2004 Microsoft Corp.
Volumeinformationen werden abgerufen...
Hierdurch wird das Volume "Lokaler Datenträger(C:)" in "h:" gesichert.
Hinweis: Die Liste der Volumes für die Sicherung umfasst nicht alle Volumes,
die Komponenten des Betriebssystems enthalten. Die Sicherung kann nicht zur
Systemwiederherstellung verwendet werden. Sie können jedoch andere Elemente wied
erherstellen, deren Wiederherstellung
vom Zielmedientyp unterstützt wird.
Der Sicherungsvorgang in "H:" wird gestartet.
Eine Schattenkopie der für die Sicherung angegebenen Volumes wird erstellt...
Eine Schattenkopie der für die Sicherung angegebenen Volumes wird erstellt...
Von Volume "Lokaler Datenträger(C:)" wird eine Sicherung erstellt. Kopiert: (0%)
.
Von Volume "Lokaler Datenträger(C:)" wird eine Sicherung erstellt. Kopiert: (10%
).
Von Volume "Lokaler Datenträger(C:)" wird eine Sicherung erstellt. Kopiert: (51%
).
Von Volume "Lokaler Datenträger(C:)" wird eine Sicherung erstellt. Kopiert: (95%
).
Die Sicherung von Volume "Lokaler Datenträger(C:)" wurde abgeschlossen.
Der Sicherungsvorgang wurde abgeschlossen.
Zusammenfassung des Sicherungsvorgangs:
Die Sicherung von Volume "Lokaler Datenträger(C:)" wurde abgeschlossen.
C:\Windows\system32>

Abbildung 14.6 Durchführen einer Systemabbildsicherung mit dem Tool Wbadmin

Wie bei allen Befehlszeilenprogrammen können Sie den Befehl auch in eine Batchdatei schreiben und sie mithilfe der Windows-Aufgabenplanung nach einem Zeitplan ausführen lassen. Sie müssen die Aufgabe dabei so konfigurieren, dass sie mit administrativen Privilegien läuft. Geben Sie dazu auf der Registerkarte *Allgemein* im Eigenschaftendialogfeld der Aufgabe ein administratives Benutzerkonto an und aktivieren Sie das Kontrollkästchen *Mit höchsten Privilegien ausführen*.



Weitere Informationen Wbadmin

Weitere Informationen über das Tool Wbadmin finden Sie unter *http://technet.microsoft.com/en-us/library/cc754015.aspx*.

Aufbau einer Systemabbildsicherung

Wenn Sie eine Systemabbildsicherung ausführen, legt Windows 7 im Stammverzeichnis des Sicherungsmediums den Ordner *WindowsImageBackup* an. Innerhalb dieses Ordners erstellt es einen Ordner, der den Namen des Computers hat. Dann legt es einen Ordner namens *Catalog* an, der die Dateien *GlobalCatalog* und *BackupGlobalCatalog* sowie einen weiteren Ordner mit dem Namen *Backup <Jahr>-<Monat>-<Tag> <Uhrzeit>* enthält, in dem sich die Datenträgerabbilddatei befindet.

Um ein ganzes Volume zu sichern, legt die Systemabbildsicherung eine VHD-Abbilddatei an. VHD-Dateien wurden in Kapitel 2 ausführlich beschrieben.

Systemabbildsicherungen erstellen außerdem folgende Dateien:

- Die Datei *MediaId* im Ordner *<ComputerName>*. Sie identifiziert das Datenträgerabbild.
- Die Dateien *GlobalCatalog* und *BackupGlobalCatalog* im Ordner *Catalog*. Sie zeichnen die Versionen des Datensicherungsabbilds auf.

- XML-Dateien (Extensible Markup Language) im *Backup*-Ordner. Sie enthalten Konfigurationseinstellungen für die Sicherungsdatei.



Hinweis Complete PC-Sicherung

Eine Systemabbildsicherung wird manchmal auch als *Complete PC-Sicherung* bezeichnet, weil sie alle Dateien aus einem oder mehreren Volumes sichert. Sie müssen aber wissen, dass eine Systemabbildsicherung nur benutzt werden kann, um ein einziges Volume in einem Computer zu sichern, der mehrere enthält. Wenn Sie alle Volumes Ihres Computers mithilfe einer Systemabbildsicherung sichern, ist das Ziel normalerweise eine Netzwerkfreigabe.

Schnelltest

- Sie wollen eine Systemabbildsicherung planen, die alle 2 Wochen ausgeführt wird. Wie gehen Sie dabei vor?

Antwort zum Schnelltest

- Erstellen Sie eine Batchdatei, die mit dem Tool Wbadmin eine Systemabbildsicherung ausführt. Öffnen Sie die Aufgabenplanung in der Konsole *Computerverwaltung* und legen Sie einen Zeitplan für diese Aufgabe fest, sodass sie alle 2 Wochen am angegebenen Tag und zur angegebenen Uhrzeit gestartet wird.

Übung Konfigurieren einer Datei- und Ordnersicherung

In dieser Übung konfigurieren Sie Ihre Datensicherung so, dass alle wichtigen Dateien Ihres Computers gesichert werden. Sie sollten die Anleitung bei Bedarf so anpassen, dass auch Ihre eigenen Dateien auf dem Computer *Canberra* gesichert werden. Anschließend erstellen Sie einen Systemreparaturdatenträger.

Übung 1 Konfigurieren einer Datensicherung

In dieser Übung wählen Sie die Dateien und Ordner auf dem Computer *Canberra* aus, die regelmäßig gesichert werden sollen. Außerdem ändern Sie den Zeitplan für die Datensicherung. Die Übung setzt voraus, dass Sie bereits eine Datei- und Ordnersicherung auf *Canberra* konfiguriert haben, in der die Standardeinstellungen verwendet werden.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Öffnen Sie die Systemsteuerung, klicken Sie auf *System und Sicherheit* und dann auf *Sichern und Wiederherstellen*.
3. Klicken Sie im Fenster *Sichern und Wiederherstellen* auf *Einstellungen ändern*.



Hinweis Der Link *Einstellungen ändern*

Der Link *Einstellungen ändern* ist nur sichtbar, wenn Sie bereits einen Datensicherungszeitplan konfiguriert und eine Datensicherung ausgeführt haben. Wie weiter oben in dieser Lektion beschrieben, werden Sie dazu aufgefordert, sobald Sie die Konsole *Sichern und Wiederherstellen* zum ersten Mal öffnen.

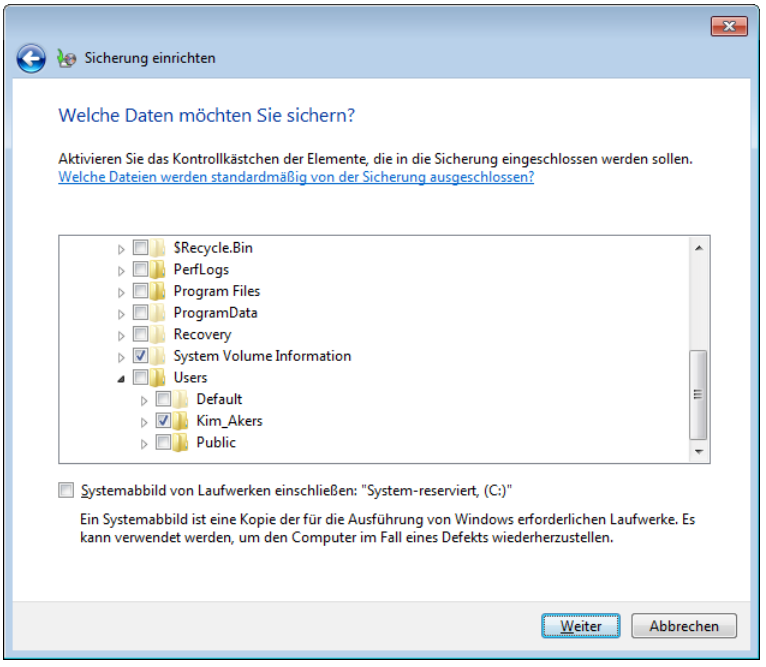

Sicherung einrichten
Welche Daten möchten Sie sichern?
Aktivieren Sie das Kontrollkästchen der Elemente, die in die Sicherung eingeschlossen werden sollen.
Welche Dateien werden standardmäßig von der Sicherung ausgeschlossen?
$Recycle.Bin
PerfLogs
Program Files
ProgramData
Recovery
System Volume Information
Users
Default
Kim_Akers
Public
Systemabbild von Laufwerken einschließen: "System-reserviert, (C:)"
Ein Systemabbild ist eine Kopie der für die Ausführung von Windows erforderlichen Laufwerke. Es kann verwendet werden, um den Computer im Fall eines Defekts wiederherzustellen.
Weiter
Abbrechen

Abbildung 14.7 Auswählen der Dateien, die gesichert werden sollen

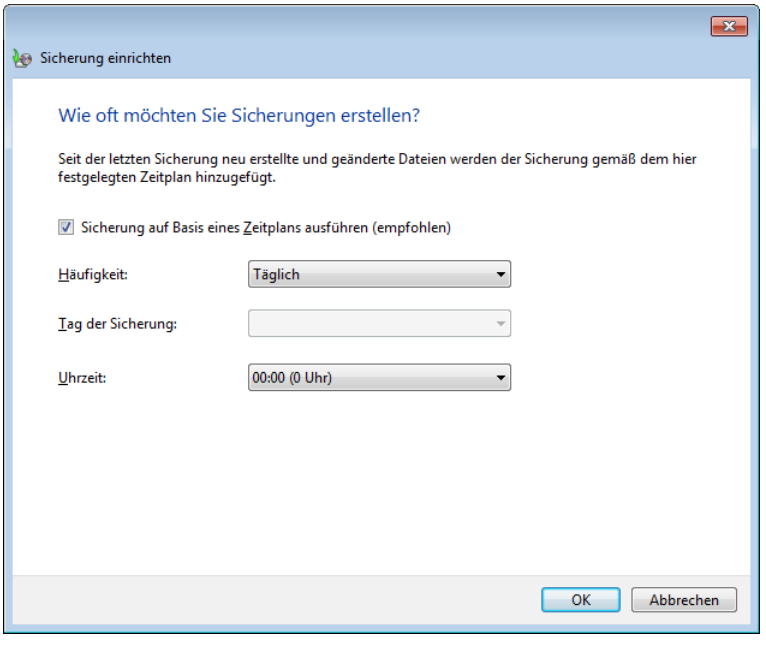

Sicherung einrichten
Wie oft möchten Sie Sicherungen erstellen?
Seit der letzten Sicherung neu erstellte und geänderte Dateien werden der Sicherung gemäß dem hier festgelegten Zeitplan hinzugefügt.
Sicherung auf Basis eines Zeitplans ausführen (empfohlen)
Häufigkeit:
Täglich
Tag der Sicherung:
Uhrzeit:
00:00 (0 Uhr)
OK
Abbrechen

Abbildung 14.8 Auswählen eines Zeitplans für die Datensicherung

4. Wählen Sie ein Zielvolume aus, zum Beispiel eine zweite interne Festplatte oder ein externes USB-Festplattenlaufwerk.
5. Klicken Sie auf *Weiter*. Wählen Sie auf der Seite *Welche Daten möchten Sie sichern* die Option *Auswahl durch Benutzer* aus. Klicken Sie auf *Weiter*.
6. Wählen Sie die Dateien aus, die Sie sichern wollen. Ihre Einstellungen sehen wahrscheinlich anders aus als in Abbildung 14.7. Aktivieren Sie nicht das Kontrollkästchen *Systemabbild von Laufwerken einschließen*.
7. Klicken Sie auf *Weiter*.
8. Klicken Sie auf der Seite *Sicherungseinstellungen überprüfen* auf *Zeitplan ändern*.
9. Richten Sie einen Zeitplan ein, bei dem die Datensicherung täglich um 0:00 Uhr (Mitternacht) ausgeführt wird (Abbildung 14.8).
10. Klicken Sie auf *OK*. Prüfen Sie Ihre Sicherungseinstellungen. Klicken Sie auf *Einstellungen speichern und Programm beenden*, wenn alles in Ordnung ist.

Übung 2 Erstellen eines Systemreparaturdatenträgers

In dieser Übung erstellen Sie einen Systemreparaturdatenträger für den Computer *Canberra*.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
2. Öffnen Sie die Systemsteuerung, klicken Sie auf *System und Sicherheit* und dann auf *Sichern und Wiederherstellen*.
3. Klicken Sie im Fenster *Sichern und Wiederherstellen* auf *Systemreparaturdatenträger erstellen*.
4. Legen Sie einen leeren DVD-Rohling in den Computer *Canberra* ein.
5. Klicken Sie auf *Datenträger erstellen*.
6. Das Dialogfeld *Systemreparaturdatenträger erstellen* zeigt an, wenn der Datenträger fertig ist (Abbildung 14.9). Klicken Sie auf *Schließen*.

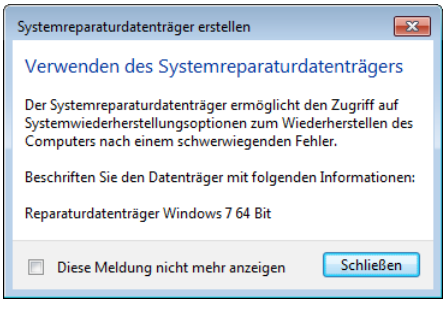

Systemreparaturdatenträger erstellen
Verwenden des Systemreparaturdatenträgers
Der Systemreparaturdatenträger ermöglicht den Zugriff auf Systemwiederherstellungsoptionen zum Wiederherstellen des Computers nach einem schwerwiegenden Fehler.
Beschriften Sie den Datenträger mit folgenden Informationen:
Reparaturdatenträger Windows 7 64 Bit
Diese Meldung nicht mehr anzeigen
Schließen

Abbildung 14.9 Erstellen eines Systemreparaturdatenträgers

Zusammenfassung der Lektion

- Sie können in der Konsole *Sichern und Wiederherstellen* einen Zeitplan für die Datei- und Ordnersicherung konfigurieren und eine solche Datensicherung sofort starten.
- Sie können in der Konsole *Sichern und Wiederherstellen* eine Systemabbildsicherung starten, aber keinen Zeitplan für eine solche Datensicherung festlegen. Es ist allerdings möglich, eine Systemabbildsicherung in der Befehlszeile zu starten und mithilfe einer Batchdatei und der Aufgabenplanung einen Zeitplan festzulegen, damit eine solche Datensicherung regelmäßig ausgeführt wird.
- Immer wenn eine Datei- und Ordnersicherung durchgeführt wird, erstellt sie einen Sicherungssatz.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 1, »Datensicherung«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Alle Clients, die im Produktivnetzwerk Ihres Unternehmens unter Windows 7 Enterprise laufen, sind so konfiguriert, dass sie jeden Sonntag um 19:00 eine Datei- und Ordnersicherung auf eine zweite interne Festplatte schreiben. Unternehmensrichtlinien schreiben für alle Computer dieselbe Einstellung vor, dass nämlich Windows auswählt, welche Dateien gesichert werden. Ein Benutzer hat auf seinem Computer einen Ordner namens *C:\Contracts* angelegt. Sie sollen sicherstellen, dass dieser Ordner und sein Inhalt gesichert werden. Welche Schritte soll der Benutzer ausführen?
   A. Er soll die Konsole *Sichern und Wiederherstellen* öffnen und auf *Einstellungen ändern* klicken. Dann soll er auf der Seite *Welche Daten möchten Sie sichern* die Option *Auswahl durch Benutzer* auswählen und den Ordner *C:\Contracts* angeben.
   B. Er soll die Konsole *Sichern und Wiederherstellen* öffnen und auf *Einstellungen ändern* klicken. Dann soll er als Datensicherungsziel eine Netzwerkfreigabe im Dateiserver des Unternehmens einstellen.
   C. Er soll den Ordner *C:\Contracts* zu seiner Bibliothek *Dokumente* hinzufügen.
   D. Er soll die Konsole *Sichern und Wiederherstellen* öffnen und auf *Jetzt sichern* klicken.
2. Ein Benutzer in Ihrem Unternehmensnetzwerk legt eine neue Datei an und bearbeitet sie den Tag über. Er speichert die Datei, entscheidet dann aber, dass er sie nicht mehr braucht, und löscht sie kurz vor Feierabend. Nachts findet eine Datei- und Ordnersicherung statt. Am nächsten Tag fällt dem Benutzer ein, dass er die Datei ja doch noch braucht. Er ruft Sie an. Was können Sie in diesem Fall tun?

A. Die Datei aus der Datensicherung der letzten Nacht wiederherstellen.
B. Den Papierkorb aus der Datensicherung der letzten Nacht wiederherstellen. Die Datei befindet sich im wiederhergestellten Papierkorb.
C. Die Datei aus einer älteren Datensicherung wiederherstellen.
D. Den Benutzer bitten, seinen Papierkorb zu öffnen.

3. Kim Akers hat ein Administratorkonto auf einem Computer mit Windows 7 Enterprise. Don Hall hat ein Standardkonto auf diesem Computer. Beide Benutzer haben Microsoft Office Word- und Microsoft Office Excel-Dateien in ihrer Bibliothek *Dokumente* abgelegt. Don speichert Microsoft Office PowerPoint-Präsentationen in einem Unterordner seiner Bibliothek *Dokumente*, der *Presentations* heißt. Außerdem speichert er Fotos in seiner Bibliothek *Bilder*. Don hat innerhalb seiner Bibliothek *Dokumente* einen Ordner namens *Secret* angelegt und diesen Ordner samt Inhalt verschlüsselt. Er speichert vertrauliche Dateien in diesem Ordner. Als Don das letzte Mal angemeldet war, hat er einige private Dateien gelöscht, aber seinen Papierkorb nicht geleert. Kim ist am Computer angemeldet. Sie hat einen USB-Flashstick angesteckt, der persönliche Dateien enthält, aber noch keine dieser Dateien auf den Computer kopiert. Sie hat das Flashspeichergerät niemals formatiert. Der Computer ist so konfiguriert, dass Windows auswählt, welche Dateien und Ordner gesichert werden. Kim öffnet die Konsole *Sichern und Wiederherstellen*, ändert aber keine Einstellungen. Sie klickt auf *Jetzt sichern*. Welche Dateien werden gesichert? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Die Word- und Excel-Dateien in Dons Bibliothek *Dokumente*
   B. Die Word- und Excel-Dateien in Kims Bibliothek *Dokumente*
   C. Die PowerPoint-Dateien in Dons Ordner *Presentations*
   D. Die Fotos in Dons Bibliothek *Bilder*
   E. Die Dateien in Dons Ordner *Secret*
   F. Die Dateien in Dons Papierkorb
   G. Die Dateien auf Kims USB-Flashstick
4. Sie haben vor Kurzem Windows 7 Ultimate auf einem Notebook installiert, Anwendungen wie Office installiert und alle ausstehenden Updates heruntergeladen und installiert. Der Computer hat zwei interne Festplatten, beide mit NTFS formatiert. Außerdem haben Sie eine externe USB-Festplatte, die Sie an das Notebook angesteckt haben. Sie führen den Befehl `convert /fs:ntfs` aus, um das externe Festplattenlaufwerk in das Dateisystem NTFS zu konvertieren. Sie haben einen 8 GByte großen USB-Flashstick, und das Notebook enthält einen DVD-Brenner. In Ihrem Büro können Sie den Computer an das Unternehmensnetzwerk anschließen und eine Verbindung zu einer Netzwerkfreigabe auf einem Dateiserver herstellen, der unter Windows Server 2008 R2 läuft. Auf welche Geräte können Sie eine vollständige Systemabbildsicherung des Systemvolumes schreiben? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Auf die zweite interne Festplatte
   B. Auf die externe Festplatte
   C. Auf das USB-Flashlaufwerk
   D. Auf mehrere DVDs
   E. In die Netzwerkfreigabe

5. Sie wollen Datensicherungen zentral durchführen, indem Sie alle Clientcomputer im Produktivnetzwerk Ihres Unternehmens in eine Netzwerkfreigabe auf einem Dateiserver sichern, der unter Windows Server 2008 R2 läuft. All Ihre Clientcomputer laufen unter Windows 7, aber weil Ihr Unternehmen mehrere Fusionen hinter sich hat, benutzen manche Windows 7 Professional, andere Windows 7 Enterprise und wieder andere Windows 7 Ultimate. Welche Computer können Sie in eine Netzwerkfreigabe sichern?
   A. Nur die Computer mit Windows 7 Ultimate
   B. Nur die Computer mit Windows 7 Enterprise
   C. Nur die Computer mit Windows 7 Ultimate oder Windows 7 Enterprise
   D. Alle Clientcomputer des Unternehmens

Lektion 2: Systemwiederherstellung

Diese Lektion beschreibt, wie Sie beschädigte oder falsch konfigurierte Systemeinstellungen in einer vorher funktionierenden Systemkonfiguration wiederherstellen. Sie stellt dabei die Themen Computerschutz, Wiederherstellungspunkte, Systemwiederherstellung und Wiederherstellen eines Systemabbilds vor.

Die Lektion beschreibt Startoptionen, erweiterte Wiederherstellungsmethoden und wie Sie vorgehen, wenn eine Systemänderung verhindert, dass Ihr Computer normal startet.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Einen Wiederherstellungspunkt von Hand erstellen
- Durchführen einer Systemwiederherstellung auf einen ausgewählten Wiederherstellungspunkt
- Durchführen einer Wiederherstellung aus einer Systemabbildsicherung
- Starten von der Windows 7-Installations-DVD und Ausführen einer Systemreparatur
- Verwenden der erweiterten Startoptionen
- Konfigurieren des Computerschutzes

Veranschlagte Zeit für diese Lektion: 30 Minuten

Durchführen einer Systemwiederherstellung

Windows 7 legt in regelmäßigen Abständen sowie vor Ereignissen wie der Installation von Anwendungen und Treibern Systemwiederherstellungspunkte an. Ein *Wiederherstellungspunkt* (restore point) enthält Informationen über Registrierungseinstellungen und andere Systeminformationen. Windows 7 generiert Wiederherstellungspunkte automatisch, bevor es größere Änderungen am System vornimmt. Sie können Wiederherstellungspunkte manuell erstellen und ein Computersystem aus einem ausgewählten Wiederherstellungspunkt wiederherstellen.

Wenn Sie eine Anwendung oder einen Treiber installieren und Ihr Computer danach instabil ist, sollten Sie erst versuchen, die Anwendung zu deinstallieren beziehungsweise die Vorversion des Treibers wiederherzustellen. Wird das Problem dadurch nicht beseitigt, können Sie Systemdateien und -einstellungen wiederherstellen, indem Sie eine Systemwiederherstellung durchführen. Dabei setzen Sie den Computer auf den Zustand zurück, den er bei seinem letzten Systemwiederherstellungspunkt hatte. Eine *Systemwiederherstellung* (system restore) setzt ein Computersystem auf den Zustand eines ausgewählten Wiederherstellungspunkts zurück. Systemwiederherstellungen ändern nichts an den Benutzerdateien. Beachten Sie, dass eine Systemwiederherstellung etwas anderes ist als eine Systemabbildwiederherstellung (system image restore), die weiter unten in dieser Lektion beschrieben wird.

Am einfachsten starten Sie eine Systemwiederherstellung, indem Sie im Suchfeld des Startmenüs **Systemwiederherstellung** eingeben und auf den entsprechenden Link klicken. In der Systemsteuerung können Sie alle Systemsteuerungselemente anzeigen, auf *Wiederherstellung* und dann auf *Systemwiederherstellung öffnen* klicken. Außerdem können Sie eine Systemwiederherstellung auf der Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften* starten. Das tun Sie in den Übungen am Ende dieser Lektion. Wenn Sie den Computer vom Installationsmedium starten, können Sie *Computer reparieren* und dann die Option

Systemwiederherstellung auswählen. Sie brauchen Administratorprivilegien, um eine Systemwiederherstellung auszuführen. Abbildung 14.10 zeigt den Assistenten *Systemwiederherstellung*.

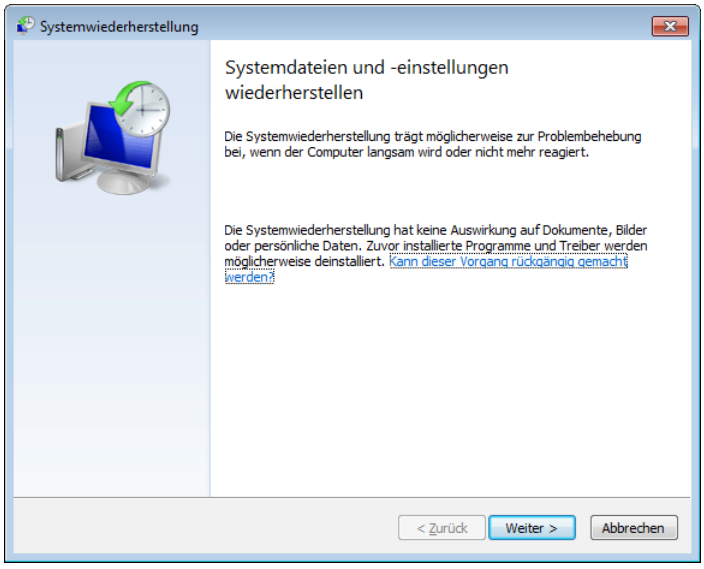

Systemwiederherstellung
Systemdateien und -einstellungen wiederherstellen
Die Systemwiederherstellung trägt möglicherweise zur Problembehebung bei, wenn der Computer langsam wird oder nicht mehr reagiert.
Die Systemwiederherstellung hat keine Auswirkung auf Dokumente, Bilder oder persönliche Daten. Zuvor installierte Programme und Treiber werden möglicherweise deinstalliert. Kann dieser Vorgang rückgängig gemacht werden?
< Zurück
Weiter >
Abbrechen

Abbildung 14.10 Der Assistent *Systemwiederherstellung*

Wenn Sie nach einem normalen Start oder einem Start, bei dem Sie die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* ausgewählt haben, eine Systemwiederherstellung durchführen, wird ein Wiederherstellungspunkt erstellt, sodass Sie die Änderungen rückgängig machen können, falls es Ihnen nicht gelingt, das Problem zu beseitigen. Führen Sie dagegen eine Systemwiederherstellung durch, während der Computer im abgesicherten Modus läuft, oder indem Sie die Systemwiederherstellungsoptionen verwenden, können Sie die Wiederherstellungsoperation nicht rückgängig machen. Wenn Sie in diesem Fall Ihre Probleme nicht beseitigen können, haben Sie die Möglichkeit, eine weitere Systemwiederherstellung durchzuführen und diesmal einen anderen Wiederherstellungspunkt zu wählen.

Eine Systemwiederherstellung stellt Windows-Systemdateien, -Programme und Registrierungseinstellungen wieder her. Sie kann außerdem Änderungen an Skripts, Batchdateien und anderen Typen ausführbarer Dateien vornehmen, die von beliebigen Benutzern Ihres Computers erstellt wurden. Eine Systemwiederherstellung hat keine Auswirkung auf persönliche Dateien, sie hilft Ihnen folglich auch nicht dabei, eine gelöschte Datei wiederherzustellen. Wenn Benutzerdokumente hinzugefügt oder geändert wurden, seit der letzte Wiederherstellungspunkt aufgezeichnet worden ist, gehen diese Änderungen andererseits auch nicht verloren, wenn Sie eine Systemwiederherstellung ausführen. Falls Sie persönliche Dateien wiederherstellen müssen, können Sie dazu die Datei- und Ordnersicherung verwenden. Und wenn Sie die Vorgängerversionen persönlicher Dateien brauchen, können Sie das Feature *Vorgängerversionen wiederherstellen* nutzen, wie in Lektion 3 beschrieben.

Der Assistent *Systemwiederherstellung* empfiehlt automatisch den neusten Wiederherstellungspunkt, der vor einer größeren Änderung erstellt wurde, etwa einer Softwareinstallation. Sie können auch in der Liste der Wiederherstellungspunkte einen auswählen. Microsoft

empfiehlt, Wiederherstellungspunkte zu verwenden, die möglichst kurz vor dem Zeitpunkt erstellt wurden, bevor Ihnen Probleme aufgefallen sind. Die Beschreibungen der automatisch erstellten Wiederherstellungspunkte geben den Namen eines Ereignisses wider, beispielsweise eine Updateinstallation mit Windows Update. Eine Systemwiederherstellung versetzt Ihren Computer in den Zustand zurück, den er vor dem gewählten Wiederherstellungspunkt hatte.

Schnelltest

- Unter welchen Voraussetzungen können Sie eine Systemwiederherstellung rückgängig machen?

Antwort zum Schnelltest

- Wenn Sie Windows 7 normal oder mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* starten und anschließend eine Systemwiederherstellung durchführen, wird ein Wiederherstellungspunkt erstellt, sodass Sie die Systemwiederherstellung rückgängig machen können.

Windows 7 reserviert Festplattenplatz für Systemwiederherstellungen. Es werden so lange Wiederherstellungspunkte gespeichert, bis dieser Festplattenplatz aufgebraucht ist. Werden danach weitere Wiederherstellungspunkte erstellt, werden alte gelöscht. Wenn Sie den Computerschutz für einen Datenträger ausschalten (das Feature, das Wiederherstellungspunkte erstellt), werden alle Wiederherstellungspunkte von diesem Datenträger gelöscht. Wenn Sie den Computerschutz später wieder einschalten, werden neue Wiederherstellungspunkte erstellt. Damit die Systemwiederherstellung wirksam ist, müssen Sie sicherstellen, dass der Computerschutz aktiviert und mindestens 300 MByte auf Ihrer Festplatte frei ist. Beseitigt eine Systemwiederherstellung Ihr Problem nicht, sollten Sie eine der erweiterten Wiederherstellungsmethoden probieren.



Hinweis Kleine Festplatten

Falls Ihre Festplatte kleiner ist als 300 MByte, brauchen Sie 50 MByte freien Platz, damit eine Systemwiederherstellung funktioniert. Festplatten dieser Größe werden allerdings immer seltener.

Computerschutz

Der Computerschutz (system protection) erstellt und speichert regelmäßig Informationen über die Systemdateien und Einstellungen Ihres Computers. Außerdem speichert er die Vorgängerversionen von Dateien, die Sie geändert haben. Er speichert diese Dateien in Wiederherstellungspunkten, die unmittelbar vor größeren Systemereignissen wie der Installation eines Programms oder Gerätetreibers erstellt werden. Wiederherstellungspunkte werden auch automatisch alle 7 Tage erstellt, sofern während der letzten 7 Tage keine anderen Wiederherstellungspunkte aufgezeichnet wurden. Schließlich haben Sie auch noch die Möglichkeit, Wiederherstellungspunkte jederzeit von Hand zu erstellen.

Der Computerschutz wird automatisch für das Laufwerk durchgeführt, auf dem das Betriebssystem gespeichert ist. Für weitere Laufwerke kann er nur aktiviert werden, wenn diese Laufwerke mit NTFS formatiert sind. Das ermöglicht Ihnen, die Systemwiederherstellung

zu benutzen und Vorgängerversionen von Dateien wiederherzustellen. In den Übungen weiter unten in dieser Lektion konfigurieren Sie den Computerschutz, erstellen einen Wiederherstellungspunkt und führen eine Systemwiederherstellung durch.

Erweiterte Wiederherstellungsmethoden

Die erweiterten Methoden stehen zur Verfügung, wenn Sie in der Systemsteuerung alle Elemente anzeigen, auf *Wiederherstellung* klicken und dann im Fenster *Wiederherstellung* auf *Erweiterte Wiederherstellungsmethoden* klicken. Sie können Windows damit in einen funktionierenden Zustand zurückversetzen, falls es schwer beschädigt ist. Abbildung 14.11 zeigt das Dialogfeld *Erweiterte Wiederherstellungsmethoden*.

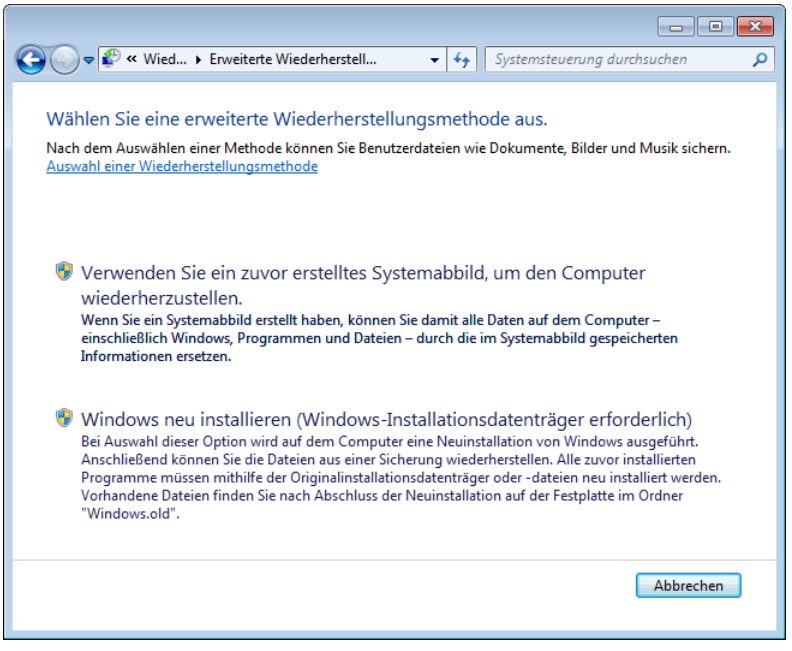

« Wied... ▸ Erweiterte Wiederherstell...
Systemsteuerung durchsuchen
Wählen Sie eine erweiterte Wiederherstellungsmethode aus.
Nach dem Auswählen einer Methode können Sie Benutzerdateien wie Dokumente, Bilder und Musik sichern.
Auswahl einer Wiederherstellungsmethode
Verwenden Sie ein zuvor erstelltes Systemabbild, um den Computer wiederherzustellen.
Wenn Sie ein Systemabbild erstellt haben, können Sie damit alle Daten auf dem Computer – einschließlich Windows, Programmen und Dateien – durch die im Systemabbild gespeicherten Informationen ersetzen.
Windows neu installieren (Windows-Installationsdatenträger erforderlich)
Bei Auswahl dieser Option wird auf dem Computer eine Neuinstallation von Windows ausgeführt. Anschließend können Sie die Dateien aus einer Sicherung wiederherstellen. Alle zuvor installierten Programme müssen mithilfe der Originalinstallationsdatenträger oder -dateien neu installiert werden. Vorhandene Dateien finden Sie nach Abschluss der Neuinstallation auf der Festplatte im Ordner "Windows.old".
Abbrechen

Abbildung 14.11 Das Dialogfeld *Erweiterte Wiederherstellungsmethoden*

Die erste Methode benutzt eine Systemabbildsicherung, die in Lektion 1 beschrieben wurde. Die zweite Methode installiert Windows neu, entweder aus einem Wiederherstellungsabbild, das von Ihrem Computerhersteller zur Verfügung gestellt wird, oder aus den Windows-Originaldateien. Beide Methoden können dazu führen, dass Daten verloren gehen. Bevor Sie eine dieser Methoden starten, werden Sie aufgefordert, Ihre persönlichen Dateien an einem externen Speicherort zu sichern, beispielsweise auf einer USB-Festplatte. Das Vorgehen beim Wiederherstellen aus einer Systemabbildsicherung ist im nächsten Abschnitt beschrieben. Beachten Sie, dass die Wiederherstellung aus einer Systemabbildsicherung etwas anderes ist als das Durchführen einer Systemwiederherstellung.

Wiederherstellen aus einer Systemabbildsicherung

Eine Systemabbildwiederherstellung überschreibt den gesamten Inhalt des Systemvolumes. Daher führen Sie eine Wiederherstellung aus einer Systemabbildsicherung durch, indem Sie Windows 7 von der Installations-DVD starten und die Systemwiederherstellungstools laden oder während des Startprozesses F8 drücken. Mithilfe der Wiederherstellung aus einer Sys-

temabbildsicherung können Sie einen Computer schnell wieder zum Laufen bekommen, nachdem Sie eine defekte Festplatte ausgetauscht haben oder die Betriebssysteminstallation beschädigt wurde (beispielsweise durch Malware, die sich nur durch vollständiges Löschen der Festplatten zuverlässig beseitigen lässt). Diese Methode wird manchmal auch als *vollständige Wiederherstellung* (complete recovery) oder *Complete PC-Wiederherstellung* (complete PC restore) bezeichnet.

Bei diesem Vorgang wird vorausgesetzt, dass die Dateien der Systemwiederherstellungsoptionen (auch als Windows-Wiederherstellungsumgebung, Windows Recovery Environment oder Windows RE bezeichnet) auf der Festplatte vorhanden sind. Ist das nicht der Fall, können Sie das System von der Installations-DVD starten und während des Systemstarts F8 drücken, um auf die erweiterten Startoptionen zuzugreifen. Dies wird im nächsten Abschnitt dieser Lektion beschrieben.

Gehen Sie folgendermaßen vor, um eine Systemabbildsicherung wiederherzustellen:

1. Stellen Sie sicher, dass das Datensicherungsmedium an Ihren Computer angeschlossen ist.
2. Legen Sie die Windows 7-DVD ein. Stellen Sie sicher, dass das Computer-BIOS so konfiguriert ist, dass von der DVD gestartet wird.
3. Starten Sie Ihren Computer neu. Drücken Sie irgendeine Taste, wenn gefragt wird, ob von DVD gestartet werden soll.
4. Windows 7-Setup wird geladen. Wählen Sie das gewünschte Gebietsschema aus, wenn Sie dazu aufgefordert werden, und klicken Sie auf *Weiter*.
5. Klicken Sie auf *Computer reparieren*.
6. Klicken Sie im Dialogfeld *Systemwiederherstellungsoptionen* auf *Systemabbild-Wiederherstellung*. Falls die Datensicherung auf eine DVD geschrieben wurde, müssen Sie diese DVD jetzt einlegen. Klicken Sie auf *Weiter*. Der Windows-Systemabbild-Wiederherstellungs-Assistent startet.
7. Auf der Seite *Systemabbildsicherung auswählen* ist automatisch die neuste Datensicherung ausgewählt. Klicken Sie auf *Weiter*, wenn Sie diese Datensicherung für die Wiederherstellung verwenden wollen. Wählen Sie andernfalls die Option *Systemabbild auswählen*, klicken Sie auf *Weiter* und wählen Sie auf der nächsten Seite die gewünschte Datensicherung.
8. Aktivieren Sie auf der Seite *Weitere Wiederherstellungsoptionen auswählen* das Kontrollkästchen *Datenträger formatieren und neu partitionieren*, wenn Sie die Festplatte neu formatieren und alle Daten darauf überschreiben wollen oder wenn die Festplatte noch nicht formatiert ist. Wenn Sie nicht alle Daten auf Ihrer aktuellen Festplatte überschreiben wollen, dürfen Sie dieses Kontrollkästchen nicht aktivieren. Klicken Sie auf *Weiter*.
9. Klicken Sie auf *Fertig stellen* und dann auf *Ja*, um die Wiederherstellung zu bestätigen.

Die Windows-Systemabbildwiederherstellung liest die Daten aus der Datensicherung und überschreibt die vorhandenen Dateien. Eine solche Wiederherstellung dauert üblicherweise zwischen 30 und 60 Sekunden pro GByte. Sie können die Wiederherstellung auf einer unterschiedlich großen Festplatte ausführen, sofern sie genug Platz zum Speichern der Datensicherung hat. Sobald die Wiederherstellung abgeschlossen ist, wird der Computer vom wiederhergestellten Systemvolume neu gestartet.

Erweiterte Startoptionen und Systemwiederherstellungsoptionen

Auf einem Windows 7-Computer greifen Sie auf die erweiterten Startoptionen zu, indem Sie den Computer neu starten und die Taste F8 gedrückt halten, während er startet. Sie können das unabhängig davon tun, ob Sie von der Installations-DVD oder von Festplatte starten. So haben Sie die Möglichkeit, auf Reparaturtools wie die Systemwiederherstellung zuzugreifen, wenn fehlerhafte Änderungen am System dazu führen, dass der Computer nicht mehr von seinem Systemvolume startet. Sie haben anschließend die Auswahl zwischen folgenden Optionen:

- **Abgesicherter Modus** Lädt einen minimalen Satz Treiber.
- **Abgesicherter Modus mit Netzwerktreibern** Lädt nur die Treiber, die unbedingt gebraucht werden, um grundlegende Funktionen und Netzwerkkonnektivität zu ermöglichen.
- **Abgesicherter Modus mit Eingabeaufforderung** Lädt nur einen minimalen Satz Treiber und startet Windows 7 mit einer Befehlszeilenoberfläche.
- **Startprotokollierung aktivieren** Zeichnet Details über den Startprozess auf. Dabei wird eine Datei namens *Ntbtlog.txt* erstellt, die alle Treiber auflistet, die während des Systemstarts geladen wurden. Hier ist zu erkennen, welche Datei zuletzt geladen wurde, als ein Fehler auftrat.
- **Anzeige mit niedriger Auflösung aktivieren (640x480)** Lädt nur Standardtreiber für den Bildschirm. Verwenden Sie diese Option, wenn Sie einen neuen Grafikkartentreiber installiert haben und jetzt keine lesbare Anzeige mehr bekommen.
- **Letzte als funktionierend bekannte Konfiguration (erweitert)** Startet den Computer mit der letzten Konfiguration, von der bekannt ist, dass sie funktioniert hat.
- **Verzeichnisdienstwiederherstellung** Bei einem Clientcomputer ist diese Option nicht von Bedeutung.
- **Debugmodus** Aktiviert das Kerneldebuggen und die Systemabbildwiederherstellung.
- **Automatischen Neustart bei Systemfehler deaktivieren** Ermöglicht Ihnen, die Informationen auf einem blauen STOP-Bildschirm zu lesen, die andernfalls verschwinden, sobald der Computer neu startet.
- **Erzwingen der Treibersignatur deaktivieren** Erlaubt Ihnen, unsignierte Treiber zu laden.
- **Windows normal starten** Versucht, Windows 7 normal zu starten. Wenn Sie den Computer von der Installations-DVD gestartet haben, wird nach dem Auswählen dieser Option Setup gestartet, sodass die Windows 7-Installation beginnt.

Die letzte als funktionierend bekannte Konfiguration wird weiter unten in dieser Lektion beschrieben. Der Debugmodus startet den Kerneldebugger. Wenn Sie diese Option auswählen, wird Windows PE (Windows Preinstallation Environment) geladen, woraufhin die Systemwiederherstellungsoptionen (auch als Windows RE bezeichnet) starten.

Systemwiederherstellungsoptionen

Wenn Sie in den erweiterten Startoptionen *Debugmodus* auswählen, werden Sie im Dialogfeld *Systemwiederherstellungsoptionen* aufgefordert, eine Tastatureingabemethode auszuwählen (normalerweise Ihre deutsche Standardtastatur). Anschließend bekommen Sie zwei Möglichkeiten zur Auswahl angeboten:

- *Verwenden Sie Wiederherstellungstools, mit denen sich Probleme beim Starten von Windows beheben lassen*
- *Stellen Sie den Computer mithilfe eines zuvor erstellten Systemabbilds wieder her*

Mit der zweiten Option starten Sie die Systemabbildwiederherstellung, wie weiter oben in dieser Lektion beschrieben. Dies ist in Windows 7 das Gegenstück zur Complete PC-Wiederherstellung von älteren Betriebssystemen (in Hilfedateien und der Microsoft TechNet-Dokumentation wird auch noch oft dieser Begriff verwendet).

Wenn Sie die erste Option auswählen, werden Sie aufgefordert, ein Betriebssystem zu wählen, das repariert werden soll (sofern mehrere vorhanden sind). Wenn Sie auf *Weiter* klicken, öffnet sich ein Dialogfeld, das der Optionsauswahl der Windows-Wiederherstellungsumgebung in älteren Betriebssystemen ähnelt. Hier stehen folgende Möglichkeiten zur Auswahl:

- **Systemstartreparatur** Behebt automatisch Probleme, die verhindern, dass Windows startet. Falls bei einem früheren Neustart von Windows 7 Probleme aufgetreten sind, erhalten Sie bei einem normalen Start (ohne dass Sie auf die erweiterten Startoptionen zugreifen) die Möglichkeit, die Systemstartreparatur auszuwählen. Abbildung 14.12 zeigt den Bildschirm, der in dieser Situation geöffnet wird.


Windows-Fehlerbehebung
Windows konnte nicht gestartet werden. Dies kann auf eine kürzlich durchgeführte Hardware- oder Softwareänderung zurückzuführen sein.
Wenn Windows-Dateien beschädigt oder falsch konfiguriert wurden, kann die Starthilfe zum Diagnostizieren und Beheben des Problems verwendet werden.
Wählen Sie "Windows normal starten", wenn die Stromversorgung während des Startes unterbrochen wurde.
(Wählen Sie eine Option mit den Pfeiltasten aus.)
Starthilfe starten (empfohlen)
Windows normal starten
Beschreibung: Startet Windows mit normalen Einstellungen.
EINGABETASTE=Auswählen

Abbildung 14.12 Die Option zum Starten der Systemstartreparatur

- **Systemwiederherstellung** Bietet eine weitere Methode, eine Systemwiederherstellung aus einem Wiederherstellungspunkt durchzuführen, wie weiter oben in dieser Lektion beschrieben. Weil Sie auf dieses Menü zugreifen können, wenn Sie von einer DVD starten, können Sie Ihr System reparieren, wenn kürzliche Änderungen an Systemeinstellungen verhindern, dass Ihr Computer normal startet.
- **Systemabbild-Wiederherstellung** Hier können Sie eine Systemabbildwiederherstellung durchführen. Diese Option wählen Sie, wenn Ihre Festplatte defekt war oder vollständig gelöscht werden musste. Falls Systemänderungen Probleme verursachen, sollten Sie die Option *Systemwiederherstellung* versuchen.

- **Windows-Speicherdiagnose** Analysiert den Arbeitsspeicher (RAM) des Computers, um Hardwareprobleme zu erkennen.
- **Eingabeaufforderung** Gibt Ihnen in einer Befehlszeilenschnittstelle Zugriff auf Dateisystem, Volumes und Dateien.



Hinweis Benutzen der Wiederherstellungstools

Wenn Windows RE auf Ihrer Installations-DVD enthalten ist, können Sie vom Windows 7-Installationsmedium starten, die Option *Computer reparieren* wählen und dann mithilfe der Wiederherstellungstools auf die Systemwiederherstellungsoptionen zugreifen. Die vorher beschriebene Methode (Drücken von F8) steht Ihnen aber immer offen, unabhängig davon, ob die Windows RE-Dateien auf Ihrer DVD vorhanden sind und ob Sie von Ihrer Installations-DVD oder von Festplatte starten.

Schnelltest

- Sie wählen in den erweiterten Startoptionen die Option *Startprotokollierung aktivieren* aus. Welche Datei wird dadurch erstellt und welche Informationen werden darin gespeichert?

Antwort zum Schnelltest

- Bei der Startprotokollierung wird eine Datei namens *Ntbtlog.txt* erstellt. Sie listet alle Treiber auf, die während des Systemstarts geladen werden, darunter die Datei, die zuletzt geladen wurde, bevor ein Fehler auftrat.

Die letzte als funktionierend bekannte Konfiguration

Die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* in den erweiterten Startoptionen ist eine Wiederherstellungsmethode, bei der Sie Ihren Computer mit den letzten Einstellungen starten, die noch funktioniert haben. Bei der letzten als funktionierend bekannten Konfiguration werden die Registrierungsdaten und Treibereinstellungen wiederhergestellt, die wirksam waren, als der Computer das letzte Mal erfolgreich gestartet wurde.

Sie sollten die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* verwenden, wenn Sie Windows 7 nicht mehr starten können, nachdem Sie eine Änderung an Ihrem Computer vorgenommen haben, oder wenn Sie den Verdacht haben, dass eine Änderung, die Sie gerade durchgeführt haben, ein Problem verursacht. Dieser Fall kann beispielsweise eintreten, wenn Windows nicht mehr startet, nachdem Sie einen neuen Grafikkartentreiber installiert haben. Wenn Sie Ihren Computer mit der letzten als funktionierend bekannten Konfiguration starten, verwendet Windows 7 die Konfiguration, die im folgenden Registrierungsschlüssel gespeichert ist:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet
```

Abbildung 14.13 zeigt den Schlüssel *Control* innerhalb des Registrierungsschlüssels *CurrentControlSet*. Sobald Ihr Computer neu startet und Sie sich anmelden, wird die aktuelle Konfiguration aus *ControlSet001* in *CurrentControlSet* kopiert, sodass sie die letzte als funktionierend bekannte Konfiguration wird. Passen Sie daher auf, wenn Sie bemerken, dass Meldungen über Fehlerereignisse in die Ereignisanzeige geschrieben werden, während Ihr Anmeldebildschirm aktiv ist. Falls Sie sich an diesem Punkt anmelden, können Sie nicht zur

letzten als funktionierend bekannten Konfiguration zurückkehren. Es ist allerdings möglich, eine Systemwiederherstellung mit einem älteren Wiederherstellungspunkt durchzuführen.

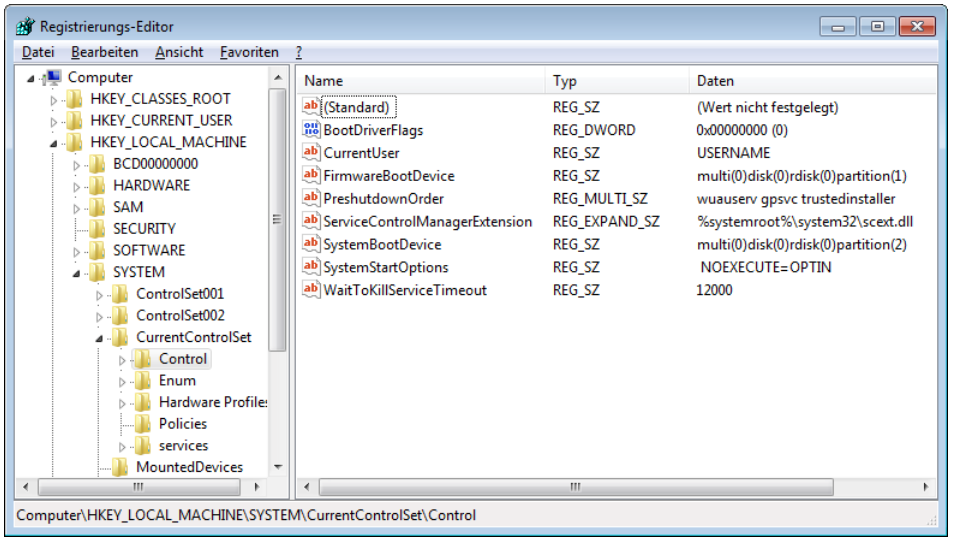


Abbildung 14.13 Der Registrierungsschlüssel *CurrentControlSet*

Systemstartoptionen in Windows 7

Windows 7 enthält ein Startladeprogramm, eine Systemstartkonfiguration und ein Speicherungssystem, das als Startkonfigurationsdaten (Boot Configuration Data, BCD) bezeichnet wird, sowie ein Tool zum Bearbeiten von Startoptionen, das BCDEdit heißt. In Kapitel 2 haben Sie erfahren, wie Sie VHDs auf Computern, die unter Windows 7 Enterprise oder Ultimate Edition laufen, mit dem Tool BCDEdit startfähig machen.

Windows 7 stellt folgende Startladeprogrammfeatures zur Verfügung:

- Windows-Start-Manager (*Bootmgr.exe*)
- Windows-Betriebssystemladeprogramm (*Winload.exe*)
- Windows-Fortsetzungsladeprogramm (*Winresume.exe*)

Wenn ein Computer mit mehreren Starteinträgen zumindest einen Eintrag für Windows 7 hat, startet der Windows-Start-Manager das System und wickelt die Interaktion mit dem Benutzer ab. Es zeigt das Systemstartmenü an, lädt das ausgewählte systemspezifische Startladeprogramm und übergibt die Systemstartparameter an das Startladeprogramm.

Startkonfigurationsdaten

In Windows 7 sind Startoptionen und BCD im BCD-Speicher abgelegt. BCD stellt allen Windows 7-Computern eine einheitliche Schnittstelle zur Verfügung, und Administratoren können damit Rechte zum Verwalten von Startoptionen zuweisen. BCD steht während der Laufzeit und aller Phasen des Setups zur Verfügung, auch beim Aufwecken des Computers aus dem Ruhezustand.

Sie können BCD mit dem Tool BCDEdit im Remotezugriff verwalten. Außerdem können Sie BCD verwalten, während das System von einem anderen Medium startet als dem, auf

dem der BCD-Speicher liegt. Dieses Feature ist wichtig für das Debuggen und die Problembehandlung, besonders wenn ein BCD-Speicher wiederhergestellt werden muss, während die Systemstartreparatur von DVD, von einem USB-Speicherstick oder im Remotezugriff ausgeführt wird. Zum Beispiel erzwingt der folgende Befehl beim Neustart die Verwendung des VGA-Anzeigetreibers (Video Graphics Array):

```
bcdedit /set vga on
```

Der nächste Befehl aktiviert den Kerneldebugger für den aktuellen Betriebssystemstarteintrag:

```
bcdedit /debug on
```

Der folgende Befehl deaktiviert den Kerneldebugger für einen Betriebssystemstarteintrag, der anhand seiner GUID (Global Unique Identifier) angegeben wird:

```
bcdedit /debug <GUID> off
```

Sie können mit dem Tool BCDEdit folgende Aufgaben ausführen:

- Erstellen eines BCD-Speichers
- Neuerstellen des BCD-Speichers
- Hinzufügen von Einträgen zu einem vorhandenen BCD-Speicher
- Ändern vorhandener Einträge in einem BCD-Speicher
- Löschen von Einträgen aus einem BCD-Speicher
- Exportieren von Einträgen aus einem BCD-Speicher
- Importieren von Einträgen in einen BCD-Speicher
- Auflisten der momentan aktiven Einstellungen
- Abfragen aller Einträge eines bestimmten Typs
- Übernehmen einer globalen Änderung für alle Einträge
- Ändern der Standardwerte für eine Zeitüberschreitung



Weitere Informationen BCD-Startoptionen

Weitere Informationen über BCD-Startoptionen finden Sie unter *http://msdn.microsoft.com/en-us/library/aa906217.aspx*.

Sie können das Tool BCDEdit benutzen, um Startoptionen in Windows 7 zu bearbeiten. Sie müssen Mitglied der lokalen Gruppe *Administratoren* sein, wenn Sie BCDEdit verwenden wollen. Sie können auch die WMI-Schnittstelle (Windows Management Instrumentation) nutzen, um vom Programmcode aus die Startoptionen zu ändern. Kapitel 13, »Überwachung und Leistung«, beschreibt WMI genauer.



Weitere Informationen Die WMI-Schnittstelle von BCD

Weitere Informationen über die WMI-Schnittstelle von BCD und das Windows Software Development Kit (SDK) enthält *http://msdn.microsoft.com/en-us/library/aa362692.aspx*.

Wiederherstellen der Vorversion eines Treibers

Manchmal treten Probleme auf, weil ein neu installierter Treiber für ein Hardwaregerät zu anderen Treibern oder zur Hardware in Ihrem Computer inkompatibel ist. Ein klassischer Fall ist, wenn Sie einen Grafikkartentreiber aktualisieren und dann nach dem Neustart des Computers feststellen müssen, dass kein Bild mehr angezeigt wird.

In diesem Fall müssen Sie Ihren Computer in den Zustand zurückversetzen, in dem er war, bevor Sie den Treiber aktualisiert haben. Sofern Sie sich noch nicht angemeldet haben, seit der Treiber aktualisiert wurde, können Sie die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* in den erweiterten Startoptionen auswählen. Ist das nicht möglich, sollten Sie probieren, eine Systemwiederherstellung durchzuführen.

Üblicherweise öffnen Sie die erweiterten Startoptionen, indem Sie die Taste F8 drücken und *Debugmodus* wählen oder von DVD starten und *Computer reparieren* wählen. In beiden Fällen wählen Sie die Option *Systemwiederherstellung* und stellen Ihre Systemeinstellungen aus dem Systemwiederherstellungspunkt wieder her, der angelegt wurde, bevor Sie den problematischen Treiber installiert haben. Es empfiehlt sich, immer einen Systemwiederherstellungspunkt aufzuzeichnen, bevor Sie größere Änderungen an einem Computer vornehmen (beispielsweise einen neuen Treiber installieren).

Es ist aber nicht immer bequem, die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* zu wählen oder eine Systemwiederherstellung durchzuführen. Vielleicht wurde der Treiber über Windows Update zusammen mit anderen wichtigen und empfohlenen Updates installiert, die Sie nicht rückgängig machen wollen. In diesem Fall müssen Sie den Computer entweder mit der Option *Abgesicherter Modus* oder *Anzeige mit niedriger Auflösung aktivieren (640x480)* starten (wenn das Problem ein Grafikkartentreiber ist) und die Vorversion des Treibers wiederherstellen. Das Verwalten von Treibern im Geräte-Manager wurde in Kapitel 4, »Verwalten von Geräten und Datenträgern«, ausführlich beschrieben.

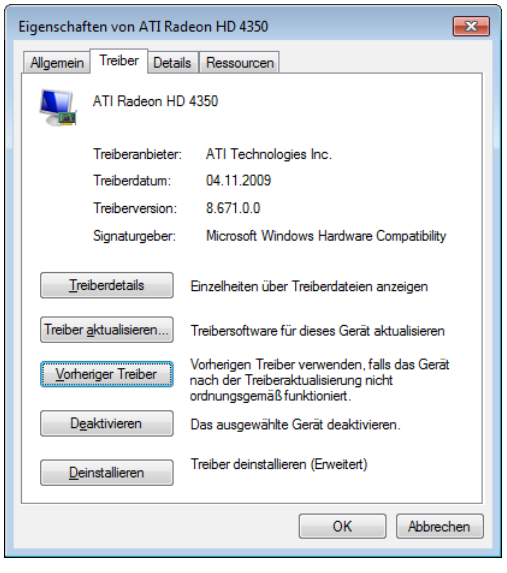


Abbildung 14.14 Die Registerkarte *Treiber* im Eigenschaftendialogfeld eines Geräts

Auf der Registerkarte *Treiber* im Eigenschaftendialogfeld des Geräts (Abbildung 14.14) können Sie den Treiber deinstallieren oder deaktivieren. Falls das Gerät ein Monitor ist, führt das unter Umständen dazu, dass der Treiber für eine geringe Standardauflösung verwendet wird. Bei anderen Geräten ist die Folge oft, dass das Gerät überhaupt nicht mehr funktioniert.

Daher sollten Sie nach Möglichkeit den vorherigen Treiber wiederherstellen. Damit wird die Vorversion des Treibers wiederhergestellt, die benutzt wurde (und einwandfrei funktioniert hat), bevor der neue Gerätetreiber installiert wurde. Eine der Hauptaufgaben der Optionen *Abgesicherter Modus* und *Anzeige mit niedriger Auflösung aktivieren (640x480)* besteht darin, Ihnen zu ermöglichen, Änderungen an Gerätetreibern vorzunehmen, die Probleme verursachen. Beachten Sie, dass die Schaltfläche *Vorheriger Treiber* nur verfügbar ist, wenn ein Treiber für das Gerät installiert wurde, der den vorherigen Treiber ersetzt.

Übung Konfigurieren des Computerschutzes, Erstellen eines Wiederherstellungspunkts und Durchführen einer Systemwiederherstellung

In dieser Übung konfigurieren Sie den Computerschutz auf einer Festplatte, auf der er in der Standardeinstellung nicht aktiviert ist. Dann erstellen Sie von Hand einen Wiederherstellungspunkt. Sie nehmen eine Änderung am System vor (durch Deinstallieren eines Treibers) und führen anschließend eine Systemwiederherstellung aus dem Wiederherstellungspunkt aus, den Sie vorher erstellt haben. Zuletzt prüfen Sie, ob die Systemänderung rückgängig gemacht wurde.

Übung 1 Konfigurieren des Computerschutzes

In dieser Übung konfigurieren Sie den Computerschutz auf einer Festplatte, die keine Systempartition enthält. Daher ist der Computerschutz dort in der Standardeinstellung nicht aktiviert. Sie können dafür eine beliebige Festplatte verwenden, ideal ist eine zweite interne Festplatte, sofern Sie eine in Ihrem Computer haben. Falls Sie Ihre Datensicherungen auf einer externen Festplatte speichern, können Sie diese Festplatte verwenden, sofern sie mit NTFS formatiert ist. In der Praxis werden Sie den Computerschutz allerdings kaum auf einem Gerät aktivieren, das nur dazu dient, Datensicherungen zu speichern. Die Konfiguration des Computerschutzes wird in Lektion 3 ausführlicher beschrieben. Gehen Sie folgendermaßen vor:

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann im Fenster *System und Sicherheit* auf *System*.
3. Klicken Sie im Fenster *System* auf Computerschutz. Daraufhin öffnet sich die Registerkarte *Computerschutz* im Dialogfeld *Systemeigenschaften* (Abbildung 14.15).
4. Wählen Sie das Laufwerk aus, für das Sie den Computerschutz konfigurieren wollen, und klicken Sie auf *Konfigurieren*.
5. Wählen Sie im Dialogfeld *Systemschutz* des ausgewählten Laufwerks die Option *Systemeinstellungen und vorherige Dateiversionen wiederherstellen* aus. Stellen Sie unter *Maximale Belegung* mit dem Schieberegler ein, wie viel Platz Sie auf der Festplatte zum Speichern von Wiederherstellungspunkten verwenden möchten (Abbildung 14.16).

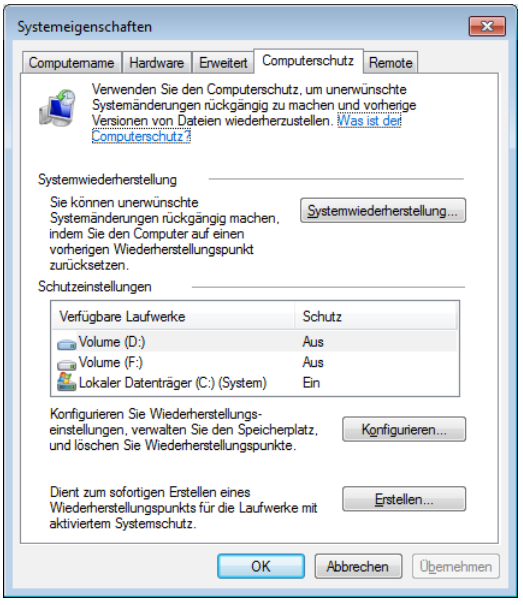


Abbildung 14.15 Die Registerkarte *Computerschutz* im Dialogfeld *Systemeigenschaften*

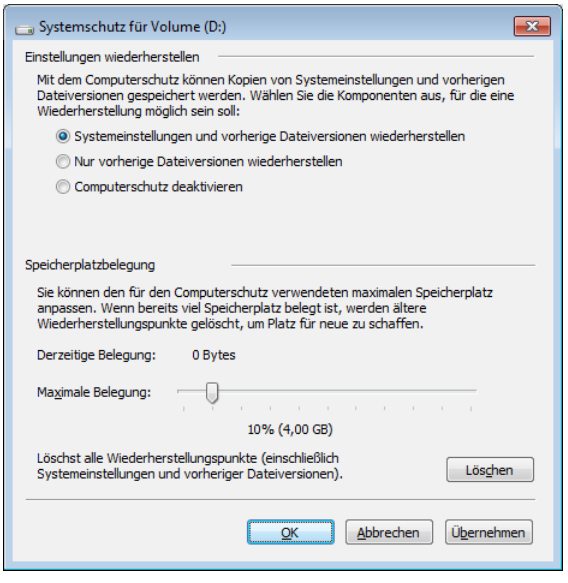

Systemschutz für Volume (D:)
Einstellungen wiederherstellen
Mit dem Computerschutz können Kopien von Systemeinstellungen und vorherigen Dateiversionen gespeichert werden. Wählen Sie die Komponenten aus, für die eine Wiederherstellung möglich sein soll:
Systemeinstellungen und vorherige Dateiversionen wiederherstellen
Nur vorherige Dateiversionen wiederherstellen
Computerschutz deaktivieren
Speicherplatzbelegung
Sie können den für den Computerschutz verwendeten maximalen Speicherplatz anpassen. Wenn bereits viel Speicherplatz belegt ist, werden ältere Wiederherstellungspunkte gelöscht, um Platz für neue zu schaffen.
Derzeitige Belegung: 0 Bytes
Maximale Belegung:
10% (4,00 GB)
Löschst alle Wiederherstellungspunkte (einschließlich Systemeinstellungen und vorheriger Dateiversionen).
Löschen
OK
Abbrechen
Übernehmen

Abbildung 14.16 Konfigurieren des Computerschutzes für ein ausgewähltes Festplattenlaufwerk

6. Klicken Sie auf *OK*.
7. Stellen Sie auf der Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften* sicher, dass in der Spalte *Schutz* für das ausgewählte Festplattenlaufwerk *Ein* angezeigt wird. Klicken Sie auf *OK*.

Übung 2 Einen Wiederherstellungspunkt von Hand erstellen

In dieser Übung erstellen Sie von Hand einen Wiederherstellungspunkt, dem Sie den Namen *Testwiederherstellungspunkt* zuweisen.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen. Öffnen Sie die Registerkarte *Computerschutz* im Dialogfeld *Systemeigenschaften*, wie in Übung 1 beschrieben.
2. Klicken Sie auf *Erstellen*.
3. Geben Sie im Dialogfeld *Wiederherstellungspunkt erstellen* den Namen **Testwiederherstellungspunkt** ein und klicken Sie auf *Erstellen*. Windows 7 legt nun den Wiederherstellungspunkt an. Das kann einige Zeit dauern.
4. Klicken Sie auf *Schließen*.

Übung 3 Durchführen einer Systemwiederherstellung

In dieser Übung nehmen Sie eine Änderung am System vor. Dann führen Sie eine Systemwiederherstellung aus Ihrem Testwiederherstellungspunkt durch und prüfen, ob die Systemänderung rückgängig gemacht wurde.

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen.
2. Klicken Sie im Startmenü mit der rechten Maustaste auf *Computer* und wählen Sie den Befehl *Verwalten*.
3. Wählen Sie im linken Fensterabschnitt der Konsole *Computerverwaltung* den Zweig *Geräte-Manager* aus.
4. Wählen Sie ein Gerät aus, das Sie momentan nicht benutzen. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie den Befehl *Eigenschaften*.

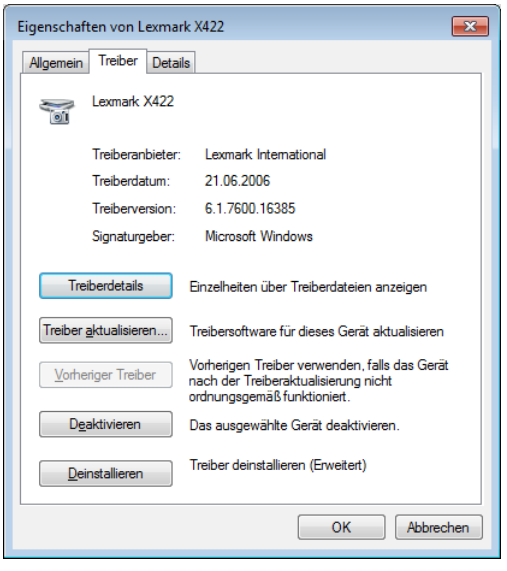


Abbildung 14.17 Die Registerkarte *Treiber* des ausgewählten Geräts

5. Aktivieren Sie die Registerkarte *Treiber* (Abbildung 14.17).
6. Klicken Sie auf *Deinstallieren*. Klicken Sie auf *OK*, um zu bestätigen, dass Sie den Treiber deinstallieren wollen.
7. Öffnen Sie erneut die Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften*, wie in Übung 1 beschrieben.
8. Klicken Sie auf *Systemwiederherstellung*.
9. Klicken Sie auf der Seite *Systemdateien und -einstellungen wiederherstellen* des Assistenten *Systemwiederherstellung* auf *Weiter*.
10. Stellen Sie auf der Seite *Wiederherstellung des Computerzustands zum angegebenen Zeitpunkt* sicher, dass *Testwiederherstellungspunkt* ausgewählt ist (Abbildung 14.18). Klicken Sie auf *Weiter*.

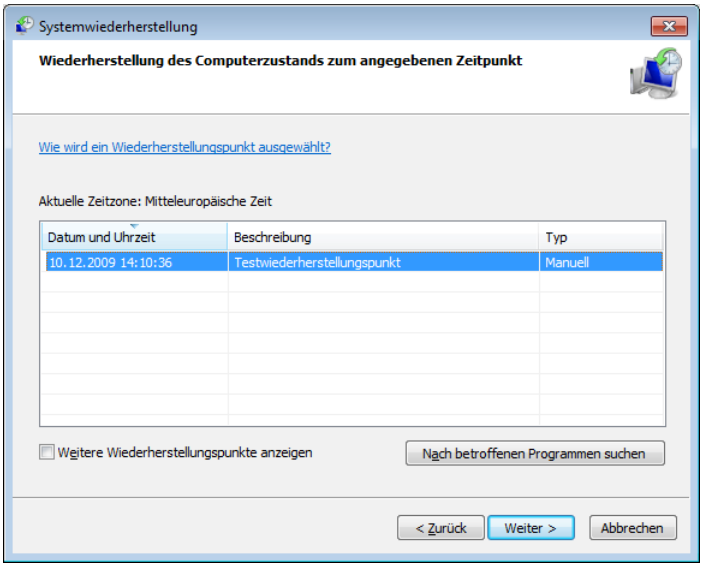


Abbildung 14.18 Auswählen eines Wiederherstellungspunkts



Warnung Ihr Computer wird neu gestartet

Im nächsten Schritt dieser Übung wird Ihr Computer neu gestartet. Stellen Sie sicher, dass Sie alle bearbeiteten Dokumente gespeichert haben und alle Anwendungen, die Sie momentan nicht benutzen, geschlossen sind.

11. Klicken Sie auf *Fertig stellen*. Klicken Sie auf *Ja*, um zu bestätigen, dass Sie die Systemwiederherstellung fortsetzen wollen. Windows 7 führt nun die Systemwiederherstellung durch, danach startet der Computer *Canberra* neu.
12. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an.
13. Klicken Sie auf *Schließen*, um das Meldungsfeld *Systemwiederherstellung* zu schließen.
14. Öffnen Sie die Registerkarte *Treiber* des Geräts, das Sie in den Schritten 4 bis 6 dieser Übung deinstalliert haben.

15. Prüfen Sie, ob der Gerätetreiber wieder installiert ist (die Schaltfläche *Deinstallieren* muss also aktiviert sein).

Zusammenfassung der Lektion

- Wenn der Computerschutz auf einem Festplattenlaufwerk konfiguriert ist, werden automatisch Wiederherstellungspunkte erstellt, sobald Sie größere Systemänderungen vornehmen. Sie können auch von Hand einen Wiederherstellungspunkt erstellen.
- Sie können Ihre Systemeinstellungen auf einen ausgewählten Wiederherstellungspunkt zurücksetzen.
- Sie können Ihren gesamten Computer aus einer Systemabbildsicherung in dem Zustand wiederherstellen, in dem er war, als die Datensicherung durchgeführt wurde.
- Sie können von der Windows 7-Installations-DVD starten und eine Systemreparatur durchführen oder die erweiterten Startoptionen öffnen, indem Sie während eines Neustarts die Taste F8 gedrückt halten. Beide Techniken geben Ihnen Zugriff auf Tools, mit denen Sie Systemstart- und Systemprobleme untersuchen und beseitigen können.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 2, »Systemwiederherstellung«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Sie testen unsignierte Gerätetreiber auf einem Computer in einem isolierten Testnetzwerk. Sie installieren einen Grafikkartentreiber. Nach dem Neustart des Computers bleibt der Bildschirm leer. Sie starten den Computer noch einmal und drücken F8. Welche erweiterten Startoptionen können Sie auswählen, um das Problem zu beseitigen? (Wählen Sie alle zutreffenden Antworten aus.)
   A. *Abgesicherter Modus*
   B. *Startprotokollierung aktivieren*
   C. *Anzeige mit niedriger Auflösung aktivieren (640x480)*
   D. *Letzte als funktionierend bekannte Konfiguration (erweitert)*
   E. *Erzwingen der Treibersignatur deaktivieren*
2. Sie entscheiden, für welche Speichergeräte Sie den Computerschutz konfigurieren. Der Computerschutz ist auf dem Laufwerk *C:*, das Ihre Systemdateien enthält, standardmäßig aktiviert. Bei allen anderen Speichergeräten Ihres Computers ist der Computerschutz ausgeschaltet. Auf welchem der folgenden Speichergeräte können Sie den Computerschutz aktivieren? (Wählen Sie alle zutreffenden Antworten aus.)
   A. Zweite interne Festplatte (formatiert mit NTFS)
   B. Externe USB-Festplatte (formatiert mit FAT)

C. USB-Flashlaufwerk

D. DVD-Laufwerk

E. Eine bereitgestellte VHD, die Sie auf Ihrer zweiten internen Festplatte angelegt haben

3. Sie untersuchen Stabilitäts- und Systemstartprobleme auf einem Computer mit Windows 7 Enterprise. Sie starten mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* und führen eine Systemwiederherstellung aus. Das beseitigt Ihre Probleme nicht, daher wollen Sie die Systemwiederherstellung rückgängig machen. Ist das möglich, und wie begründen Sie Ihre Antwort?

   A. Nein. Sie können eine Systemwiederherstellung nur rückgängig machen, wenn Sie sie mit den Systemwiederherstellungstools starten.

   B. Nein. Sie können eine Systemwiederherstellung nur rückgängig machen, wenn Sie sie nach einem normalen Systemstart durchführen.

   C. Ja. Sie können eine Systemwiederherstellung immer rückgängig machen, unabhängig davon, wie Sie den Computer gestartet oder die Wiederherstellung ausgelöst haben.

   D. Ja. Sie können eine Systemwiederherstellung rückgängig machen, die Sie nach einem normalen Systemstart oder nach einem Start mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* durchgeführt haben.

4. Sie untersuchen Stabilitätsprobleme auf einem Computer mit Windows 7 Ultimate. Sie haben den Verdacht, dass Hardwaredefekte im RAM die Ursache sind. Sie öffnen die Systemwiederherstellungsoptionen. Welche Option hilft Ihnen wahrscheinlich, das Problem zu diagnostizieren?

   A. *Windows-Speicherdiagnose*

   B. *Systemstartreparatur*

   C. *Systemwiederherstellung*

   D. *Systemabbild-Wiederherstellung*

5. Mit welchem Befehlszeilenprogramm können Sie in Windows 7 die Systemstartoptionen bearbeiten?

   A. *Bootmgr.exe*

   B. *Winload.exe*

   C. *BCDEdit.exe*

   D. *Winresume.exe*

Lektion 3: Wiederherstellen von Dateien und Ordnern

Diese Lektion beschäftigt sich mit den Vorgängerversionen von Dateien und Ordnern, die vom Volumeschattenkopiedienst (Volume Shadow Copy Service, VSS) als Schattenkopien erstellt werden, wenn ein Wiederherstellungspunkt angefertigt wird, oder in Sicherungssätzen gespeichert sind, die von einer Datei- und Ordnersicherung erstellt werden. Sie beschreibt, wie Sie Vorgängerversionen von Dateien sogar dann wiederherstellen, wenn die Originaldateien umbenannt oder gelöscht wurden.

Die Lektion stellt die Datei- und Ordnerwiederherstellung und den Assistenten *Dateien wiederherstellen* vor und beschreibt, wie Sie mit diesem Assistenten Benutzerprofildaten wiederherstellen. Der Computerschutz wurde bereits in Lektion 2 vorgestellt, diese Lektion erklärt die Computerschutzeinstellungen genauer.

Am Ende dieser Lektion werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Wiederherstellen der Vorgängerversion einer Datei oder eines Ordners
- Wiederherstellen einer Datei und eines Ordners aus einer Datensicherung
- Wiederherstellen einer umbenannten oder gelöschten Datei
- Wiederherstellen eines Benutzerprofils

Veranschlagte Zeit für diese Lektion: 35 Minuten

Wiederherstellen beschädigter oder gelöschter Dateien aus der Vorgängerversion

Vorgängerversionen sind entweder Datensicherungen von Dateien und Ordnern, die Sie in der Konsole *Sichern und Wiederherstellen* erstellen und mit demselben Tool sowie dem Assistenten *Dateien wiederherstellen* wiederherstellen, oder es sind Schattenkopien. Solche *Schattenkopien* (shadow copy) sind Kopien von Dateien und Ordnern, die Windows 7 automatisch speichert, sobald es einen Wiederherstellungspunkt erstellt. Sie können entscheiden, ob Sie die Wiederherstellung aus einer Datensicherung oder einer Schattenkopie durchführen wollen. Die Datei, die Sie aus einer Datensicherung wiederherstellen, ist die Version, die aktuell war, als die Datensicherung angefertigt wurde. Unter Umständen haben Sie eine Schattenkopie, die neuer ist als die gesicherte Datei, vielleicht wollen Sie aber auch eine ältere Version wiederherstellen.

Sie können die Vorgängerversionen von Dateien benutzen, um beschädigte Dateien oder Dateien wiederherzustellen, die Sie oder die Benutzer, für die Sie Support leisten, versehentlich geändert oder gelöscht haben. Sie können auf Vorgängerversionen zugreifen und sie in einen anderen Speicherort schreiben oder die Vorgängerversion einer beschädigten Datei am ursprünglichen Speicherort wiederherstellen.

Wiederherstellen von Dateien und Ordnern

Windows 7 macht es einfach, Dateien und Ordner aus einer Datensicherung wiederherzustellen. Sie können eine Datei oder einen Ordner an ihrem ursprünglichen Speicherort oder einem anderen Speicherort wiederherstellen. Meist stellen Sie eine Datei am ursprünglichen Speicherort wieder her, falls sie beschädigt oder versehentlich überschrieben wurde. Gelegentlich ist es allerdings sinnvoll, sie an einem anderen Speicherort wiederherzustellen, um

zu prüfen, ob Ihre Datensicherungs- und Wiederherstellungsabläufe funktionieren, ohne zu riskieren, dass Ihre richtigen Dateien und Ordner überschrieben werden. Dies wird als *Dummywiederherstellung* (dummy restore) bezeichnet.

Sie stellen eine Datei oder einen Ordner aus einer Datensicherung wieder her, indem Sie in der Konsole *Sichern und Wiederherstellen* auf *Eigene Dateien wiederherstellen* klicken. In der Standardeinstellung werden Dateien und Ordner aus der neusten Datensicherung wiederhergestellt. Wenn Sie eine ältere Datensicherung verwenden wollen, müssen Sie auf *Anderes Datum auswählen* klicken und Datum und Uhrzeit aus der Liste auswählen. Klicken Sie zuletzt auf *OK*.

Auf der ersten Seite im Assistenten *Dateien wiederherstellen* haben Sie die Möglichkeit, auf *Suchen* zu klicken und den Datei- oder Ordnernamen ganz oder teilweise einzugeben, auf *Nach Dateien suchen* zu klicken und eine Datei auszuwählen, oder auf *Nach Ordnern suchen* zu klicken und einen Ordner auszuwählen. Wählen Sie eine Datei oder einen Ordner aus und klicken Sie auf *Datei hinzufügen* beziehungsweise *Ordner hinzufügen*. Abbildung 14.19 zeigt, wie eine Datei für die Wiederherstellung ausgewählt wird.

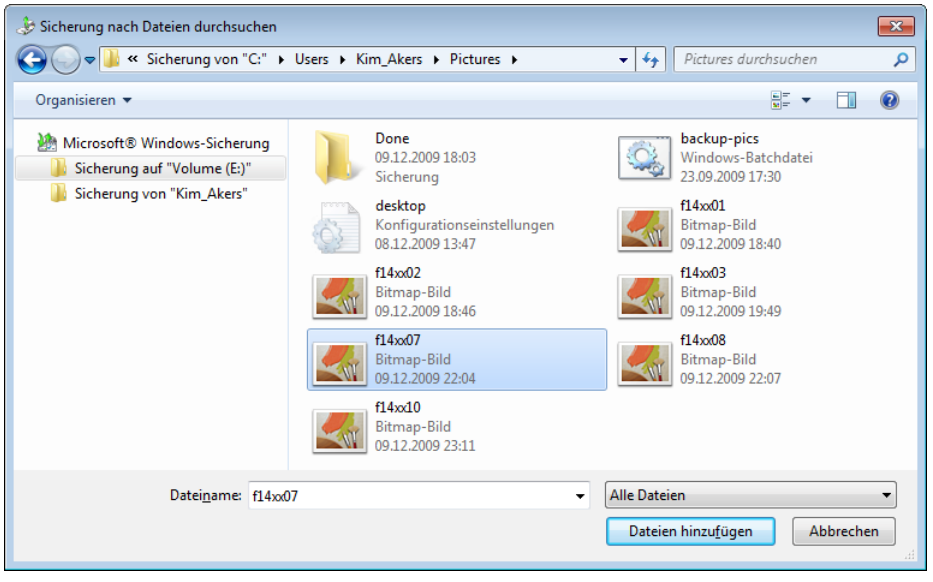


Abbildung 14.19 Auswählen einer Datei, die wiederhergestellt werden soll

Wenn Sie im Assistenten *Dateien wiederherstellen* die Dateien oder Ordner ausgewählt haben, die Sie wiederherstellen wollen, klicken Sie auf *Weiter*. Nun entscheiden Sie, ob Sie die gewählten Elemente am ursprünglichen Speicherort wiederherstellen oder einen anderen Speicherort angeben, um eine Dummywiederherstellung durchzuführen. Sie können den Pfad für die Dummywiederherstellung direkt eingeben oder danach suchen. Der Speicherort für die Dummywiederherstellung kann auf einer internen oder externen Festplatte, einem USB-Flashstick, einem optischen Laufwerk, einer VHD oder (nur in Windows 7 Ultimate, Enterprise und Professional Edition) einer Netzwerkfreigabe liegen.

Klicken Sie auf *Wiederherstellen*, sobald Sie angegeben haben (oder die Standardeinstellung übernommen haben), wo Ihre Dateien oder Ordner wiederhergestellt werden sollen. Gibt es am angegebenen Speicherort bereits eine Datei oder einen Ordner mit demselben Namen,

bekommen Sie die Optionen *Kopieren und ersetzen*; *Nicht kopieren* und *Kopieren, aber beide Dateien behalten* zur Auswahl angeboten (wie auch bei allen normalen Dateikopiervorgängen). Wenn Sie wollen, können Sie das Kontrollkästchen *Vorgang für alle Konflikte durchführen* aktivieren und dann auswählen, welche Aktion Windows 7 durchführen soll. Außerdem haben Sie die Möglichkeit, die gespeicherten Dateien zu überprüfen. Klicken Sie zuletzt auf *Fertig stellen*.

Schattenkopien

Schattenkopien werden automatisch gespeichert, wenn ein Wiederherstellungspunkt angelegt wird. Wenn der Computerschutz aktiviert ist, erstellt Windows 7 automatisch Schattenkopien der Dateien, die seit dem letzten Wiederherstellungspunkt geändert wurden. In der Standardeinstellung wird alle 7 Tage ein neuer Wiederherstellungspunkt erstellt, außerdem immer vor einer größeren Änderung am System (beispielsweise Treiber- oder Anwendungsinstallationen).

Sie greifen auf Vorgängerversionen einer Datei oder eines Ordners zu, indem Sie im Windows-Explorer mit der rechten Maustaste auf die Datei oder den Ordner klicken und den Befehl *Vorgängerversionen wiederherstellen* wählen. Sie bekommen dann eine Liste der verfügbaren Versionen der Datei oder des Ordners angezeigt (Abbildung 14.20). Die Liste umfasst sowohl gesicherte Dateien als auch Schattenkopien, sofern beide Typen verfügbar sind.

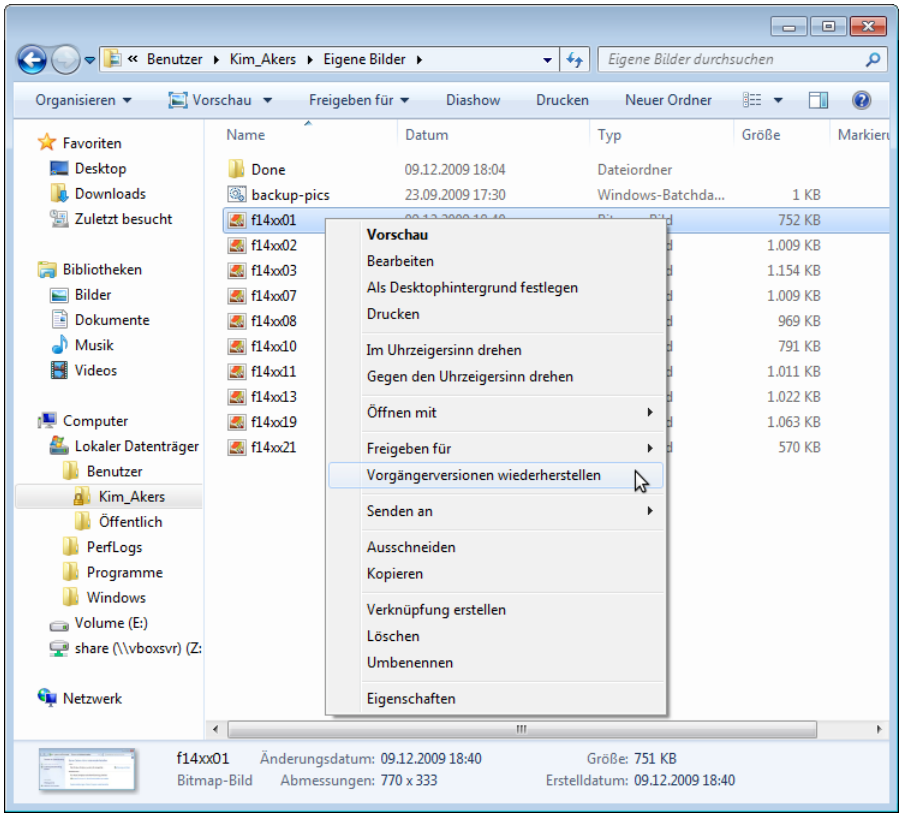


Abbildung 14.20 Auswählen des Befehls *Vorgängerversionen wiederherstellen*

Wenn Sie eine Vorgängerversion einer Datei oder eines Ordners wiederherstellen wollen, können Sie mit der rechten Maustaste darauf klicken und den Befehl *Vorgängerversionen wiederherstellen* wählen. Klicken Sie auf den Eintrag, den Sie wiederherstellen wollen, und dann auf die Schaltfläche *Wiederherstellen* (Abbildung 14.21). Sie müssen aufpassen, welche Vorgängerversion Sie wiederherstellen, denn diese Datei beziehungsweise dieser Ordner ersetzt die aktuelle Version auf dem Computer. Diese Operation können Sie nicht rückgängig machen. Falls *Wiederherstellen* nicht zur Verfügung steht, können Sie keine Vorgängerversion der Datei oder des Ordners wiederherstellen (möglicherweise weil sich die Ordnerstruktur geändert hat). Unter Umständen ist es aber möglich, die Vorgängerversion zu öffnen oder an einem anderen Speicherort zu speichern.

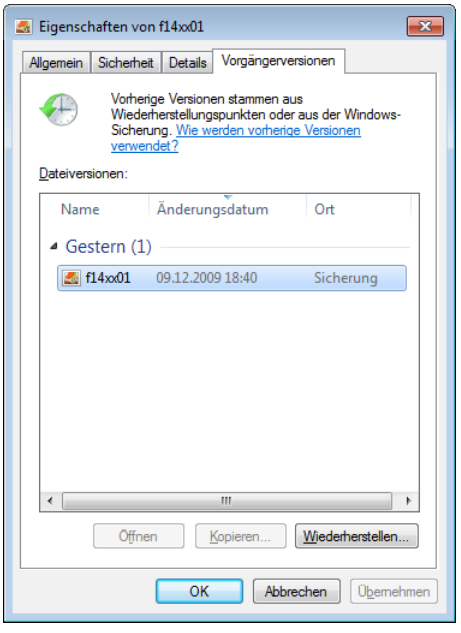


Abbildung 14.21 Auswählen einer Vorgängerversion, die wiederhergestellt werden soll

Auf der Registerkarte *Vorgängerversionen* im Eigenschaftendialogfeld einer Datei werden alle Vorgängerversionen von Dateien aufgeführt, die entweder direkt aus Wiederherstellungspunkten auf Ihrer Festplatte oder einer Datensicherung stammen. Wenn Sie eine Sicherungskopie wiederherstellen wollen, gehen Sie genauso vor. Sobald Sie in diesem Fall auf *Wiederherstellen* klicken, startet Windows 7 den Assistenten *Dateien wiederherstellen*.

Falls Sie zu einigen Dateien keine Schattenkopien finden, ist möglicherweise der Computerschutz für diese Festplatte ausgeschaltet oder die Dateien sind Offlinedateien. Offlinedateien sind Kopien von Dateien, die in einem freigegebenen Netzwerkordner gespeichert sind. Schattenkopien stehen nicht für Offlinedateien zur Verfügung. Schattenkopien stehen auch nicht für Dateien und Ordner zur Verfügung, die Windows 7 zum Ausführen benötigt. Zum Beispiel gibt es keine Schattenkopien des Systemordners (des Ordners, in dem das Betriebssystem installiert ist).

Wiederherstellen umbenannter und gelöschter Dateien

Sie können eine Datei oder einen Ordner, der gelöscht oder umbenannt wurde, aus einer Schattenkopie wiederherstellen, aber Sie müssen wissen, an welchem Speicherort die Datei oder der Ordner abgelegt war. In den Übungen am Ende dieser Lektion simulieren Sie einen solchen Fall.

Sie können eine gelöschte Datei nicht mehr direkt wiederherstellen, nachdem der Papierkorb geleert wurde. Aber Sie können eine Vorgängerversion des Ordners wiederherstellen, in dem die Datei enthalten war. Passen Sie dabei auf: Wenn Sie den Ordner wiederherstellen, werden andere Dateien in diesem Ordner durch ihre Vorgängerversionen überschrieben. Nachdem der Papierkorb geleert wurde, gehen Sie folgendermaßen vor, um eine versehentlich gelöschte Datei wiederherzustellen:

1. Stellen Sie fest, in welchem Ordner sich die gelöschte Datei befand.
2. Legen Sie einen neuen Ordner an und kopieren Sie den Inhalt des Ordners, den Sie wiederherstellen wollen, in den neuen Ordner.
3. Ersetzen Sie den Ordner, den Sie wiederherstellen wollen, durch seine neuste Vorgängerversion.
4. Kopieren Sie den Inhalt des aktuellen Ordners in den Ordner mit der Vorgängerversion. Wählen Sie dabei die Option aus, alle älteren Dateiversionen mit neueren Versionen zu überschreiben. Die Datei, die gelöscht wurde, befindet sich nun im Ordner mit der Vorgängerversion, wird aber durch die Kopieroperation nicht beeinflusst, weil sie ja im neuen Ordner gar nicht mehr vorhanden ist.
5. Schließlich können Sie den neuen Ordner löschen.

Wiederherstellen mehrerer Vorgängerversionen derselben Datei

Wenn Sie die Vorgängerversion einer Datei oder eines Ordners (die entweder aus einem Wiederherstellungspunkt oder einer Datensicherung stammt) am ursprünglichen Speicherort wiederherstellen, wird dabei die vorhandene Datei beziehungsweise der Ordner überschrieben. Falls Sie danach eine andere Vorgängerversion derselben Datei oder desselben Ordners am ursprünglichen Speicherort wiederherstellen, überschreibt sie wiederum die Version, die Sie vorher wiederhergestellt haben.

Manchmal wollen Sie mehrere Versionen derselben Datei wiederherstellen und behalten, sei es aus Neugier oder im Rahmen einer Überwachung oder Untersuchung. In diesem Fall können Sie auf der Registerkarte *Vorgängerversionen* im Eigenschaftendialogfeld der Datei oder des Ordners (siehe Abbildung 14.21 weiter oben) auf die Schaltfläche *Kopieren* klicken.

Nehmen wir an, Sie wollen mehrere Vorgängerversionen einer Datei wiederherstellen, die 4 Wochen zurückreichen. Im ersten Schritt legen Sie einen neuen Ordner an, in dem diese Dateien gespeichert werden. Dann klicken Sie mit der rechten Maustaste auf die aktuelle Datei, wählen den Befehl *Vorgängerversionen wiederherstellen*, wählen die Vorgängerversion aus, die Sie wiederherstellen wollen, und klicken auf *Kopieren*, um sie in den neuen Ordner zu kopieren (also nicht in den Ordner, der die aktuelle Version enthält). Sie benennen die wiederhergestellte Datei um, normalerweise durch Anhängen von Monat und Tag (beispielsweise *MeineDatei_7_12.docx*). Das wiederholen Sie für alle Dateien, an denen Sie interessiert sind, wobei Sie jeder einen anderen Namen geben. Das Umbenennen ist nötigt, weil alle Vorgängerversionen derselben Datei standardmäßig auch denselben Namen tragen

und Sie vermeiden müssen, dass bereits vorher wiederhergestellte Dateien überschrieben werden.

Der Volumeschattenkopiedienst

Der Volumeschattenkopiedienst (Volume Shadow Copy Service, VSS) verwaltet und implementiert Schattenkopien, die für Datensicherungen und zum Abspeichern von Vorgängerversionen benutzt werden, wenn ein Wiederherstellungspunkt generiert wird. Außerdem verwaltet er Volumesnapshots. Wenn Sie in der Konsole *Sichern und Wiederherstellen* eine Datei- und Ordnersicherung starten, erstellt VSS einen Snapshot des Volumes, das die gesicherten Dateien und Ordner enthält. Anschließend werden diese Snapshots gesichert, nicht die Originaldateien. Das beschleunigt den Sicherungsprozess, und Sie können Dateien eines Datenträgers sogar sichern, während die Dateien geöffnet sind und Sie damit arbeiten. Beachten Sie, dass der Sicherungsprozess keine Änderungen sichert, die Sie an einer offenen Datei vorgenommen haben, seit sie das letzte Mal gespeichert wurde. Die Volumeschattenkopie erstellt Volumes, die dem ursprünglichen Volume zu dem Zeitpunkt entsprechen, als die Schattenkopie angefertigt wurde.

Der Dienst *Volumeschattenkopie* ist auf allen Windows 7-Computern installiert. Wie in Abbildung 14.22 zu sehen ist, hat er den Starttyp *Manuell*. Der Dienst startet, sobald er gebraucht wird. Gelingt es nicht, den Dienst bei Bedarf zu starten, stehen keine Schattenkopien für die Datensicherung zur Verfügung, sodass die Windows-Sicherung fehlschlägt. Sie können in diesem Fall auch keine Wiederherstellungspunkte und Vorgängerversionen erstellen. Prüfen Sie in einer solchen Situation den Dienst und stellen Sie sicher, dass er nicht deaktiviert wurde.

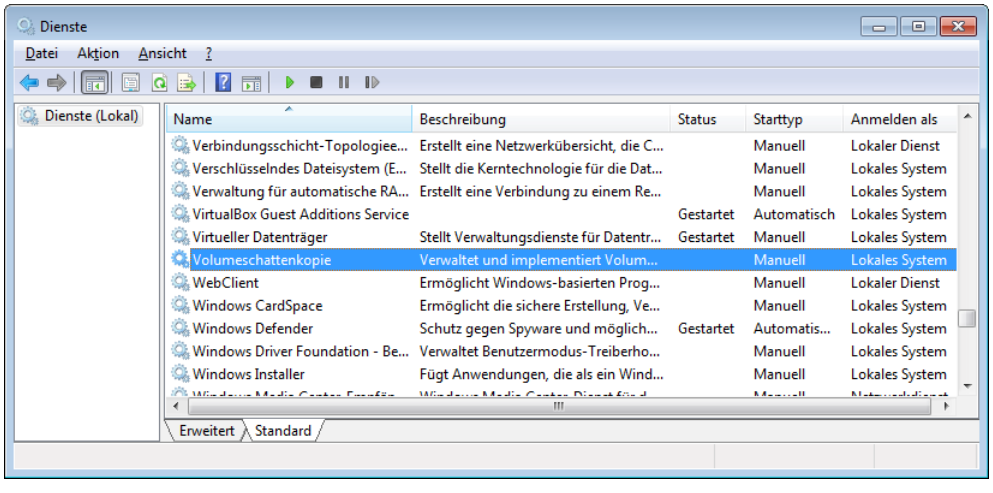

Dienste
Datei Aktion Ansicht ?
Dienste (Lokal)
Name
Beschreibung
Status
Starttyp
Anmelden als
Verbindungsschicht-Topologiee... Erstellt eine Netzwerkübersicht, die C... Manuell Lokaler Dienst
Verschlüsselndes Dateisystem (E... Stellt die Kerntechnologie für die Dat... Manuell Lokales System
Verwaltung für automatische RA... Erstellt eine Verbindung zu einem Re... Manuell Lokales System
VirtualBox Guest Additions Service Gestartet Automatisch Lokales System
Virtueller Datenträger Stellt Verwaltungsdienste für Datentr... Gestartet Manuell Lokales System
Volumeschattenkopie Verwaltet und implementiert Volum... Manuell Lokales System
WebClient Ermöglicht Windows-basierten Prog... Manuell Lokaler Dienst
Windows CardSpace Ermöglicht die sichere Erstellung, Ve... Manuell Lokales System
Windows Defender Schutz gegen Spyware und möglich... Gestartet Automatis... Lokales System
Windows Driver Foundation - Be... Verwaltet Benutzermodus-Treiberho... Manuell Lokales System
Windows Installer Fügt Anwendungen, die als ein Wind... Manuell Lokales System
Erweitert
Standard

Abbildung 14.22 Der Dienst *Volumeschattenkopie*

Wiederherstellen von Benutzerprofilen

Wenn Sie eine Datei- und Ordnersicherung ausführen, sichern Sie in der Standardeinstellung alle Dateien aller Benutzer des Computers (Bibliothek *Dokumente*, Bibliothek *Bilder*, *Favorites*-Ordner und so weiter). Daten eines bestimmten Benutzers werden als sein Benutzerprofil bezeichnet. In einem kleinen Netzwerk werden Benutzerprofile lokal gespeichert. In einem domänenbasierten, großen Unternehmensnetzwerk können Sie Benutzerprofile auf

einem Server speichern und auf einen Clientcomputer herunterladen, sobald sich ein Benutzer anmeldet. Diese Art Profil, das sogenannte *servergespeicherte Benutzerprofil* (roaming profile), ermöglicht es einem Benutzer, sich an einem beliebigen Clientcomputer innerhalb der Domäne anzumelden. Der entsprechende Computer wird dann mit seinen persönlichen Einstellungen konfiguriert und er kann auf seine Bibliotheken, Internetfavoriten, Kontakte und andere Elemente zugreifen. Wie in Abbildung 14.23 gezeigt, können Benutzerprofile eine Menge Speicherplatz verbrauchen.

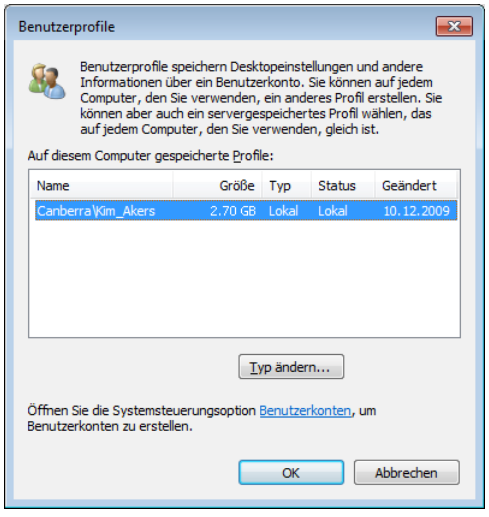

Benutzerprofile
Benutzerprofile speichern Desktopeinstellungen und andere Informationen über ein Benutzerkonto. Sie können auf jedem Computer, den Sie verwenden, ein anderes Profil erstellen. Sie können aber auch ein servergespeichertes Profil wählen, das auf jedem Computer, den Sie verwenden, gleich ist.
Auf diesem Computer gespeicherte Profile:
Name
Größe
Typ
Status
Geändert
Canberra\Kim_Akers
2.70 GB
Lokal
Lokal
10.12.2009
Typ ändern...
Öffnen Sie die Systemsteuerungsoption Benutzerkonten, um Benutzerkonten zu erstellen.
OK
Abbrechen

Abbildung 14.23 Ein Benutzerprofil, das 2,7 GByte Speicherplatz belegt

Wenn Sie kürzlich an einem Benutzerprofil vorgenommene Änderungen rückgängig machen wollen, können Sie die neuste Datensicherung des Benutzerprofils wiederherstellen, indem Sie in der Konsole *Sichern und Wiederherstellen* den Assistenten *Dateien wiederherstellen* starten. Wenn Sie ein Benutzerprofil wiederherstellen, stellen Sie normalerweise die vollständigen Ordner wieder her. Das Wiederherstellen einzelner Dateien dauert sehr lange.

Wenn Sie in der Konsole *Sichern und Wiederherstellen* auf *Eigene Dateien wiederherstellen* klicken und dann im Assistenten *Dateien wiederherstellen* die Schaltfläche *Nach Ordnern suchen* anklicken, wird im linken Fensterabschnitt des Dialogfelds *Sicherung nach Ordnern oder Laufwerken durchsuchen* zu jedem Benutzer des Computers ein eigener Ordner aufgeführt. Sobald Sie einen dieser Ordner auswählen, bekommen Sie eine Liste mit Ordnern angezeigt (Abbildung 14.24). Diese Ordner enthalten alle Dateien und Einstellungen des angegebenen Benutzers.

Wählen Sie nacheinander alle Ordner aus, die Sie wiederherstellen wollen, und klicken Sie auf *Ordner hinzufügen*. Sie müssen bei jedem Ordner, den Sie wiederherstellen, zum Dialogfeld *Sicherung nach Ordnern oder Laufwerken durchsuchen* zurückkehren. Wenn Sie alle gewünschten Ordner ausgewählt haben, müsste der Assistent *Dateien wiederherstellen* ähnlich wie in Abbildung 14.25 aussehen.

Klicken Sie nun auf *Weiter* und gehen Sie genauso vor wie bei einer normalen Datei- und Ordnerwiederherstellung. Wenn Sie beschädigte Benutzerprofildaten wiederherstellen, schreiben Sie die Daten normalerweise an den ursprünglichen Speicherort.

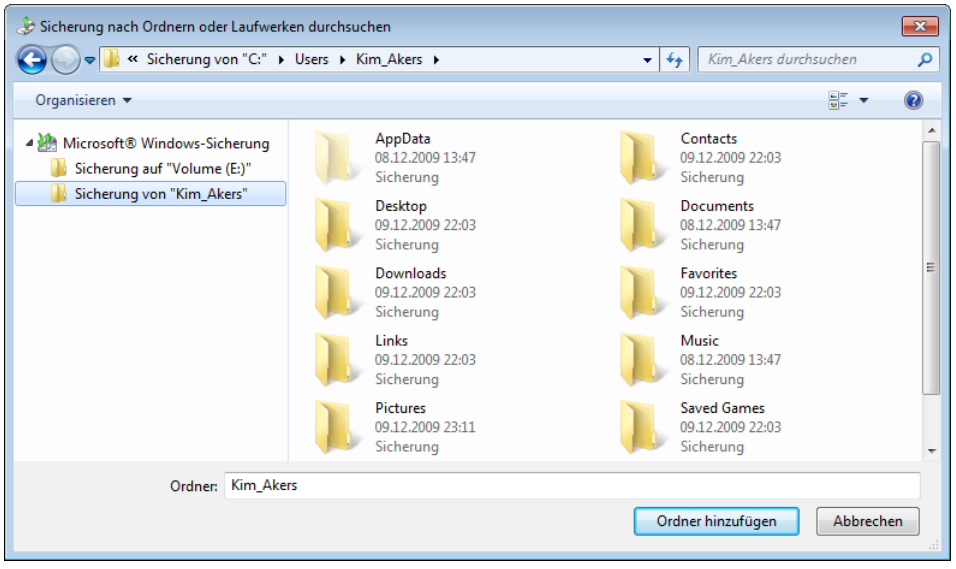


Abbildung 14.24 Datensicherung eines Benutzerprofils

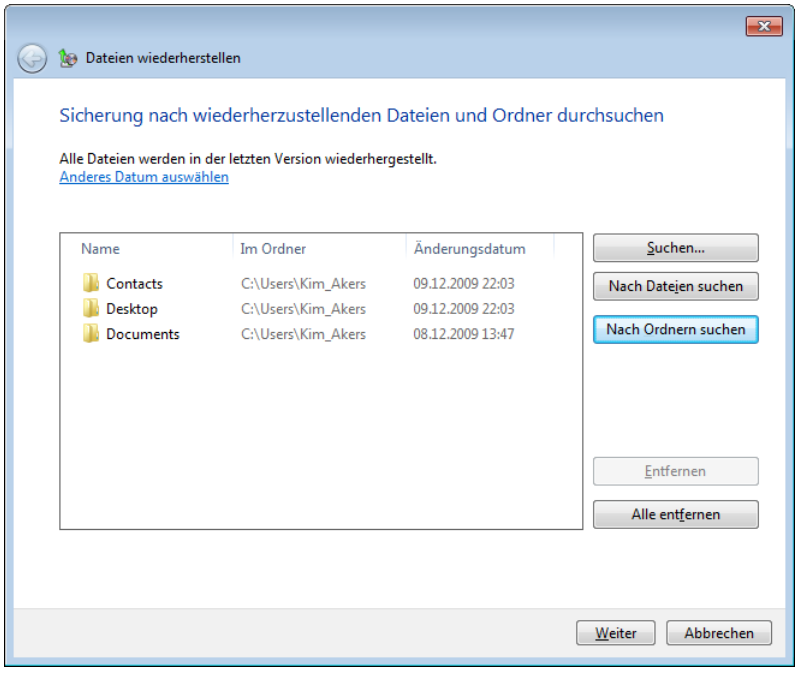


Abbildung 14.25 Auswählen, welche Benutzerprofilordner wiederhergestellt werden



Hinweis **Auswählen von Dateien**

Wenn Sie neben (oder statt) Ordnern auch eine Datei wiederherstellen wollen, können Sie auf *Nach Dateien suchen* klicken statt auf *Nach Ordnern suchen*. Sie können bei derselben Wiederherstellung sowohl Dateien als auch Ordner auswählen.

Konfigurieren von Computerschutz und Datenträgernutzung

In einer Übung von Lektion 2 haben Sie bereits die Registerkarte *Computerschutz* im Dialogfeld *Systemeigenschaften* geöffnet, um einen Wiederherstellungspunkt zu erstellen. In dieser Übung haben Sie auf *Konfigurieren* geklickt und den Computerschutz für ein Festplattenlaufwerk aktiviert. Soll ein Laufwerk in einen Wiederherstellungspunkt einbezogen werden, muss der Computerschutz dafür aktiviert sein. Das bedeutet, dass der Computerschutz auch nötig ist, damit Vorgängerversionen auf einem Laufwerk generiert werden. Auf Laufwerken, bei denen der Computerschutz nicht aktiviert ist, finden Sie keine Vorgängerversionen von Dateien und Ordnern.

In diesem Abschnitt sehen wir uns das Dialogfeld *Systemschutz* genauer an. Abbildung 14.26 zeigt dieses Dialogfeld für das Laufwerk *C:*, diese Abbildung ähnelt Abbildung 14.16 in Lektion 2 (es gibt aber Unterschiede).

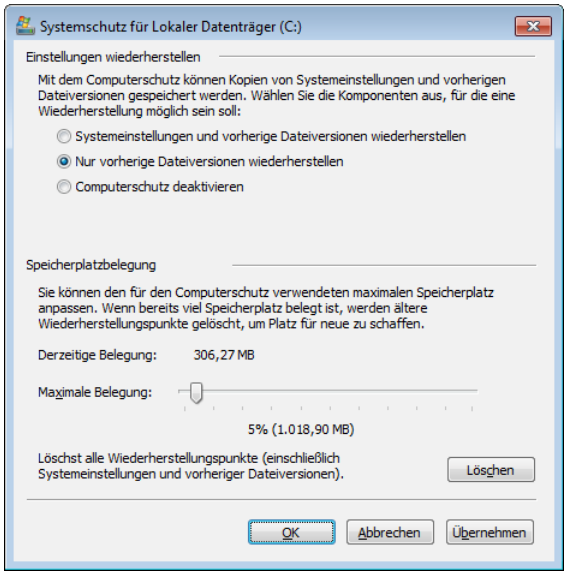

Systemschutz für Lokaler Datenträger (C:)
Einstellungen wiederherstellen
Mit dem Computerschutz können Kopien von Systemeinstellungen und vorherigen Dateiversionen gespeichert werden. Wählen Sie die Komponenten aus, für die eine Wiederherstellung möglich sein soll:
Systemeinstellungen und vorherige Dateiversionen wiederherstellen
Nur vorherige Dateiversionen wiederherstellen
Computerschutz deaktivieren
Speicherplatzbelegung
Sie können den für den Computerschutz verwendeten maximalen Speicherplatz anpassen. Wenn bereits viel Speicherplatz belegt ist, werden ältere Wiederherstellungspunkte gelöscht, um Platz für neue zu schaffen.
Derzeitige Belegung: 306,27 MB
Maximale Belegung:
5% (1.018,90 MB)
Löscht alle Wiederherstellungspunkte (einschließlich Systemeinstellungen und vorheriger Dateiversionen).
Löschen
OK
Abbrechen
Übernehmen

Abbildung 14.26 Konfigurieren des Computerschutzes

Im Abschnitt *Einstellungen wiederherstellen* [richtig: *Wiederherstellungseinstellungen*] des Dialogfelds *Systemschutz* stehen folgende Optionen zur Auswahl:

- **Systemeinstellungen und vorherige Dateiversionen wiederherstellen** Diese Option verwenden Sie normalerweise bei Festplattenlaufwerken, die ein Systemvolume enthalten. In diesem Fall ist das auch die Standardeinstellung. Auf diese Weise können Sie Wiederherstellungspunkte erstellen, die Systeminformationen speichern, die während einer Systemwiederherstellung verwendet werden. Liegen auf demselben Laufwerk auch Benutzerdateien, werden Vorgängerversionen der Dateien generiert, sobald ein Wiederherstellungspunkt erstellt wird. Normalerweise ist die Speicherplatzbelegung auf einen relativ niedrigen Wert gestellt (beispielsweise 10 Prozent), weil das Festplattenlaufwerk in erster Linie Systemdateien speichert, die nur selten aktualisiert werden.

- **Nur vorherige Dateiversionen wiederherstellen** Diese Option wählen Sie meist für Festplattenlaufwerke, die Sie zum Speichern von Dateien einsetzen, die aber keine Systemdateien enthalten. Ein typisches Beispiel ist eine zweite interne Festplatte. Wenn Sie einen Wiederherstellungspunkt erstellen, der ein Laufwerk mit dieser Computerschutzeinstellung umfasst, werden Vorgängerversionen der Dateien generiert. Normalerweise stellen Sie hier einen hohen Prozentsatz für die Speicherplatzbelegung durch den Computerschutz ein (zum Beispiel 40 Prozent), damit möglichst viele Vorgängerversionen aufbewahrt werden können.
- **Computerschutz deaktivieren** Diese Option eignet sich für Festplattenlaufwerke, die als Ziele von Datensicherungen eingesetzt werden. Sie brauchen keine Vorgängerversionen von Sicherungsdateien zu erstellen, weil die Sicherungsdateisätze diese Aufgabe schon selbst übernehmen. Üblicherweise verwenden Sie diese Einstellung für eine externe USB-Festplatte, die als Datensicherungsmedium genutzt wird.



Prüfungstipp

Denken Sie daran, dass Sie den Computerschutz nur für Festplatten (oder bereitgestellte VHDs) konfigurieren können, die mit dem Dateisystem NTFS formatiert sind. Für USB-Flashlaufwerke, optische Laufwerke oder Festplatten (interne oder externe), die mit dem Dateisystem FAT formatiert sind, können Sie den Computerschutz nicht konfigurieren und auch keine Vorgängerversionen erstellen.

Welchen Wert Sie bei der Speicherplatzbelegung konfigurieren, hängt von den persönlichen Vorlieben ab. Allgemein gilt, dass der Wert bei einem Systemdatenträger eher klein sein sollte, bei einem Datenspeicher dagegen eher groß. Ist der gesamte Platz belegt, der dem Computerschutz zugewiesen ist, werden die ältesten Vorgängerversionen überschrieben. Wenn Sie in einer Umgebung arbeiten, wo die Benutzer auf Dateiversionen zugreifen wollen, die mehrere Monate alt sind, müssen Sie unter Umständen mehr Festplattenplatz für diesen Zweck reservieren. Brauchen die Benutzer dagegen nur selten Vorgängerversionen, die älter sind als 1 Woche, können Sie sich darauf beschränken, weniger Platz zu reservieren.

Sie müssen sich auch genau überlegen, welche Option Sie für die Wiederherstellungseinstellungen auswählen. Bei einem Laufwerk, das Systemdateien enthält, verwenden Sie normalerweise *Systemeinstellungen und vorherige Dateiversionen wiederherstellen*. Aber wenn Sie einen Computer haben, der nur eine Festplatte enthält, und Sie so viele Vorgängerversionen von Dateien und Ordnern wie möglich speichern wollen, ist es unter Umständen sinnvoll, die Option *Nur vorherige Dateiversionen wiederherstellen* zu wählen. In diesem Fall müssen Sie in Kauf nehmen, dass eine Systemwiederherstellung möglicherweise nicht in der Lage ist, das Problem einer falsch konfigurierten Systemeinstellung zu beseitigen oder die Vorversion eines problematischen Treibers wiederherzustellen.



Hinweis Computerschutzeinstellungen gelten nicht rückwirkend

Falls die Vorgängerversionen von Dateien und Ordnern erst einmal gelöscht wurden, weil kein Speicherplatz mehr frei ist, werden sie nicht wiederhergestellt, wenn Sie den Wert unter *Speicherplatzbelegung* vergrößern. Wenn Sie auf die Vorgängerversion einer Datei zugreifen wollen, die vor 4 Wochen erstellt wurde, aber nur noch Vorgängerversionen vorhanden sind, die 2 Wochen zurückreichen, ist es nicht möglich, die ältere Vorgängerversionen zurückzu-

holen, indem Sie die Einstellung *Speicherplatzbelegung* ändern. Sie müssen die Datei aus dem Sicherungssatz wiederherstellen, der vor 4 Wochen erstellt wurde (oder möglichst kurz danach). Auch gesicherte Dateien sind eine Art Vorgängerversion.

Übung Wiederherstellen einer Datei, die umbenannt wurde

In dieser Übung stellen Sie die Vorgängerversion einer Datei her, die Sie umbenannt haben.

Übung Wiederherstellen einer umbenannten Datei

In dieser Übung wählen Sie eine Datei aus, von der es mehrere Vorgängerversionen gibt, und benennen sie um. Dann simulieren Sie den Fall, dass Sie eine ältere Version der Datei wiederherstellen müssen. Sie stellen die Vorgängerversion unter ihrem ursprünglichen Dateinamen wieder her. Sie benötigen keine erhöhten Privilegien, um diese Übung durchzuarbeiten. Sie werden allerdings aufgefordert, sich unter einem Administratorkonto anzumelden. Sofern Sie keine besonders gut geschulten Benutzer haben, ist es üblicherweise die Aufgabe eines Administrators, eine umbenannte Datei wiederherzustellen.

In der Übung verwenden Sie eine Datei (beispielsweise ein Word-Dokument oder eine Excel-Tabelle), die eine Reihe von Vorgängerversionen hat. Mit etwas Glück gibt es solche Dateien auf dem Computer. Falls nicht, müssen Sie eine Datei erstellen, eine Datei- und Ordnersicherung ausführen, die Datei bearbeiten und einen Wiederherstellungspunkt erstellen. Wie Sie manuelle Datensicherungen ausführen und von Hand einen Wiederherstellungspunkt erstellen, wurde weiter oben in diesem Kapitel beschrieben. Die Abbildungen in der Übung zeigen eine Beispieldatei namens *Lektion 2.txt*. Sie können selbstverständlich eine beliebige andere Datei auf Ihrem Computer *Canberra* verwenden. Gehen Sie folgendermaßen vor, um eine Vorgängerversion der umbenannten Datei wiederherzustellen:

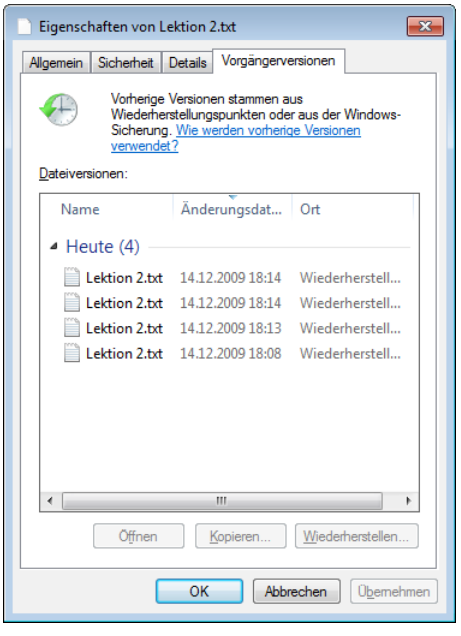


Abbildung 14.27 Vorgängerversionen einer ausgewählten Datei

1. Melden Sie sich unter dem Konto *Kim_Akers* am Computer *Canberra* an, sofern noch nicht geschehen
2. Öffnen Sie den Windows-Explorer, indem Sie im Startmenü auf *Computer* klicken.
3. Wechseln Sie in einen Ordner, in dem Sie persönliche Dateien speichern.
4. Öffnen Sie den Ordner und klicken Sie mit der rechten Maustaste auf eine Datei, die Sie regelmäßig bearbeiten. Wählen Sie *Vorgängerversionen wiederherstellen* aus.
5. Prüfen Sie, ob Vorgängerversionen der Datei vorhanden sind (Abbildung 14.27).
6. Schließen Sie das Eigenschaftendialogfeld der Datei.
7. Klicken Sie mit der rechten Maustaste auf die Datei und ändern Sie ihren Namen.
8. Klicken Sie mit der rechten Maustaste auf die umbenannte Datei und wählen Sie erneut den Befehl *Vorgängerversionen wiederherstellen*. Wie in Abbildung 14.28 zu sehen, werden keine Vorgängerversionen mehr aufgelistet.

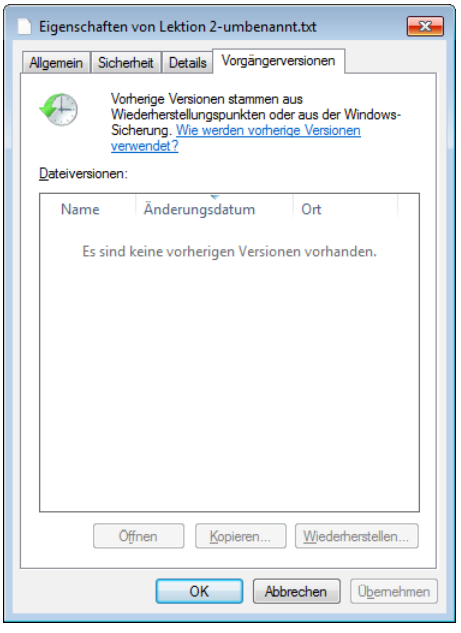


Abbildung 14.28 Es stehen keine Vorgängerversionen für die umbenannte Datei mehr zur Verfügung

9. Um eine Vorgängerversion der Datei wiederherzustellen, müssen Sie in der Ordneransicht auf der linken Seite des Windows-Explorer-Fensters mit der rechten Maustaste auf den Ordner klicken, in dem sie gespeichert ist, und den Befehl *Vorgängerversionen wiederherstellen* wählen (Abbildung 14.29).
10. Wählen Sie eine Vorgängerversion des Ordners aus, in dem die Datei, die Sie wiederherstellen wollen, wahrscheinlich enthalten ist, und klicken Sie dann auf *Öffnen* (Abbildung 14.30).

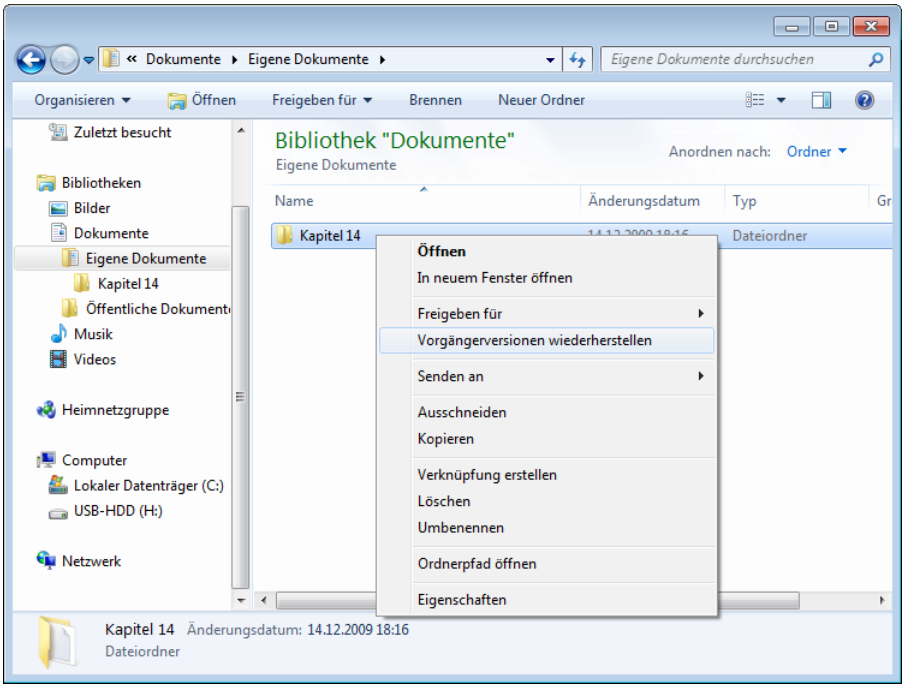


Abbildung 14.29 Wiederherstellen der Vorgängerversionen eines Ordners

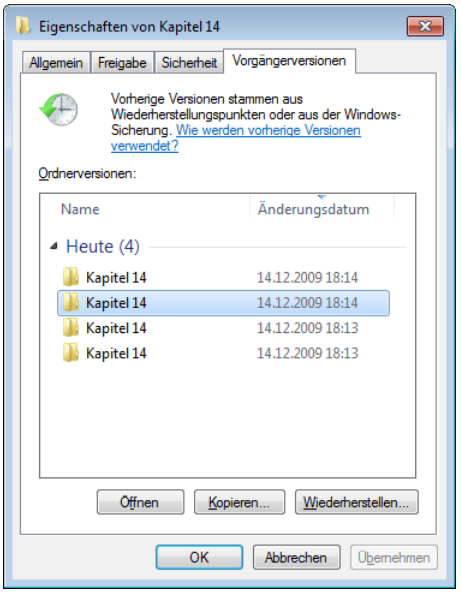


Abbildung 14.30 Auswählen der Vorgängerversion eines Ordners, der die Datei enthält, die wiederhergestellt werden soll

11. Wie in Abbildung 14.31 zu sehen, müsste die Vorgängerversion der Datei, die Sie wiederherstellen wollen, in der Vorgängerversion des Ordners liegen. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie den Befehl *Kopieren*.

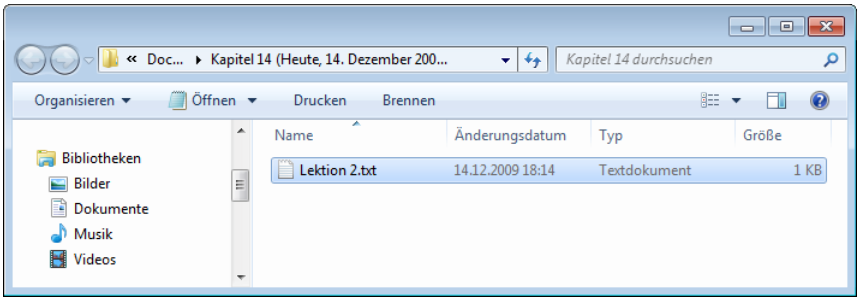


Abbildung 14.31 Die Vorgängerversion der umbenannten Datei im wiederhergestellten Ordner

12. Schließen Sie die Vorgängerversion des Ordners. Fügen Sie die Datei am gewünschten Speicherort ein. Es empfiehlt sich, sie anschließend zu öffnen und sicherzustellen, dass es die Version ist, die Sie brauchen.

Zusammenfassung der Lektion

- Sie können die Vorgängerversion einer Datei oder eines Ordner aus Schattenkopien, die beim Anlegen eines Wiederherstellungspunkts erstellt werden, oder aus Sicherungssätzen wiederherstellen.
- Sie können eine umbenannte oder gelöschte Datei wiederherstellen, indem Sie eine Vorgängerversion des Ordners wiederherstellen, in dem die ursprüngliche Datei gespeichert war.
- Sie können Benutzereinstellungen und Benutzerdaten wie Desktopeinstellungen, Kontakte und Favoriten wiederherstellen, indem Sie ein Benutzerprofil wiederherstellen.
- Sie können den Computerschutz für interne und externe Festplattenlaufwerke und VHDs konfigurieren, die mit dem Dateisystem NTFS formatiert sind. Vorgängerversionen von Dateien und Ordnern werden erstellt, wenn Sie einen Wiederherstellungspunkt auf einem Laufwerk erstellen, für das der Computerschutz eingerichtet ist.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen aus Lektion 3, »Wiederherstellen von Dateien und Ordnern«, überprüfen. Die Fragen finden Sie (in englischer Sprache) auch auf der Begleit-CD, Sie können sie also auch auf dem Computer im Rahmen eines Übungstests beantworten.



Hinweis Die Antworten

Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende des Buchs.

1. Ein Benutzer ruft Sie am Helpdesk an. Er hat versehentlich eine Datei gelöscht, die er früher an diesem Tag bearbeitet hat. Sie haben seinen Computer so konfiguriert, dass er jeden Abend eine Datensicherung ausführt. Außerdem haben Sie vor 2 Tagen einen neuen Grafikkartentreiber installiert. Wie stellen Sie die Datei des Benutzers wieder her?
   A. Öffnen Sie die Konsole *Sichern und Wiederherstellen* und stellen Sie die Datei aus der Datensicherung wieder her.
   B. Stellen Sie die Datei mit dem Feature *Vorgängerversionen wiederherstellen* wieder her.
   C. Öffnen Sie den Papierkorb, klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie den Befehl *Wiederherstellen*.
   D. Führen Sie eine Systemwiederherstellung aus.
2. Ein Angestellter, der zu Hause arbeitet, ruft Sie am Helpdesk an. Ein Virenangriff hat die einzige interne Festplatte seines Computers vollständig gelöscht. Er hat vor 3 Monaten eine Systemabbildsicherung des Computers durchgeführt und sichert seine persönlichen Dateien jede Nacht automatisch. Seine Datensicherungen speichert er auf einem externen USB-Festplattenlaufwerk, das mit dem Dateisystem NTFS formatiert ist. All seine persönlichen Dateien befinden sich in der Bibliothek *Dokumente*. Was raten Sie ihm? (Wählen Sie alle zutreffenden Antworten aus; die richtigen Antworten bilden zusammen die vollständige Lösung.)
   A. Führen Sie eine Systemabbildwiederherstellung aus.
   B. Führen Sie eine Systemwiederherstellung aus.
   C. Stellen Sie die Bibliothek *Dokumente* mit dem Feature *Vorgängerversionen wiederherstellen* aus einer Schattenkopie wieder her.
   D. Klicken Sie in der Konsole *Sichern und Wiederherstellen* auf *Eigene Dateien wiederherstellen*, um den Ordner mit der Bibliothek *Dokumente* wiederherzustellen.
3. Ihr Computer mit Windows 7 Enterprise hat zwei interne Festplatten. Auf Laufwerk *C:*, das das Betriebssystem und installierte Anwendungen enthält, ist der Computerschutz standardmäßig konfiguriert. Das Laufwerk *D:* ist eine 500-GByte-Festplatte, die mit NTFS formatiert ist; darauf speichern Sie Ihre persönlichen Dateien. Sie wollen Vorgängerversionen speichern, die mehrere Monate zurückreichen. Daher wollen Sie 200 GByte dieser Festplatte für den Computerschutz reservieren. Für die Datensicherung verwenden Sie keine dieser internen Festplatten, sondern eine 1 TByte große externe USB-Festplatte. Wie konfigurieren Sie den Computerschutz für Ihr Laufwerk *D:*? (Wählen Sie alle zutreffenden Antworten aus; die richtigen Antworten bilden zusammen die vollständige Lösung.)
   A. Wählen Sie die Option *Systemeinstellungen und vorherige Dateiversionen wiederherstellen*
   B. Wählen Sie die Option *Nur vorherige Dateiversionen wiederherstellen*
   C. Stellen Sie den Schieberegler *Maximale Belegung* auf 40 Prozent
   D. Stellen Sie den Schieberegler *Maximale Belegung* auf 4 Prozent

4. Die Chefbuchhalterin Ihres Unternehmens kommt mit einer Frage zu einer Finanztabelle zu Ihnen. Sie muss eine bestimmte, 6 Monate alte Version dieser Tabelle wiederherstellen, weil sie für eine Buchprüfung benötigt wird. Sie prüfen die Vorgängerversionen und stellen fest, dass die älteste gespeicherte Version 3 Monate alt ist. Wie können Sie die benötigte Datei wiederherstellen?
   A. Bearbeiten Sie die Computerschutzeinstellungen für das Volume, auf dem die Datei gespeichert ist. Vergrößern Sie mit dem Schieberegler *Maximale Belegung* den Prozentsatz, der auf der Festplatte für den Computerschutz reserviert ist, auf 70 Prozent.
   B. Führen Sie eine Systemwiederherstellung durch. Wählen Sie einen Systemwiederherstellungspunkt, der vor 6 Monaten erstellt wurde.
   C. Bearbeiten Sie die Computerschutzeinstellungen für das Volume, auf dem die Datei gespeichert ist. Wählen Sie die Option *Nur vorherige Dateiversionen wiederherstellen* aus.
   D. Stellen Sie die Datei in der Konsole *Sichern und Wiederherstellen* aus einem Sicherungssatz wieder her, der vor 6 Monaten gespeichert wurde.
5. Eine Benutzerin ruft bei Ihrem Helpdesk an. Ihre Favoritenliste ist beschädigt, daher ist es schwierig, auf die Websites zuzugreifen, die sie regelmäßig besucht. Bei allen Computern in Ihrem Unternehmen wird jede Nacht eine Datei- und Ordnersicherung durchgeführt, die mit den Standardeinstellungen konfiguriert ist. Auf allen Clientcomputern des Unternehmens wurde vor 24 Stunden ein Wiederherstellungspunkt erstellt, weil ein neuer Gerätetreiber installiert wurde. Und vor 3 Wochen haben Sie bei allen Computern des Unternehmens eine Systemabbildsicherung durchgeführt. Die Benutzerin kennt sich nicht mit Computern aus und bittet Sie, das Problem für sie zu lösen. Wie können Sie das am einfachsten tun?
   A. Führen Sie eine Systemwiederherstellung aus.
   B. Führen Sie eine Systemabbildwiederherstellung aus.
   C. Stellen Sie mit dem Assistenten *Dateien wiederherstellen* den Favoritenordner im gesicherten Profil der Benutzerin wieder her.
   D. Öffnen Sie im Browser der Benutzerin unter *Favoriten* die Registerkarte *Verlauf*. Kopieren Sie die zuletzt besuchten Sites und fügen Sie sie zu den Favoriten hinzu.

Zusammenfassung des Kapitels

- Sie können in der Konsole *Sichern und Wiederherstellen* einen Zeitplan für die Datei- und Ordnersicherung konfigurieren und eine solche Datensicherung sofort starten. Eine Systemabbildsicherung können Sie darin starten, aber keinen Zeitplan für eine solche Datensicherung festlegen. Sie können in einer Eingabeaufforderung mit erhöhten Rechten eine Systemabbildsicherung starten. Sie können Ihren gesamten Computer aus einer Systemabbildsicherung in dem Zustand wiederherstellen, den er hatte, als die Datensicherung durchgeführt wurde. Sie können Dateien, Ordner und Benutzerprofildaten aus den Sicherungssätzen von Datei- und Ordnersicherungen wiederherstellen.
- Wiederherstellungspunkte werden automatisch erstellt, wenn Sie größere Änderungen am System vornehmen. Sie können einen Wiederherstellungspunkt auch manuell erstellen und Ihre Systemeinstellungen aus einem ausgewählten Wiederherstellungspunkt wiederherstellen. Sie konfigurieren den Computerschutz auf einem Festplattenlaufwerk, damit Wiederherstellungspunkte erstellt werden. Dabei legen Sie fest, wie viel Platz auf der Festplatte für den Computerschutz reserviert wird.
- Mithilfe der erweiterten Startoptionen und der Systemreparatur können Sie Probleme beseitigen, wenn der Computer nicht mehr normal startet.
- Sie können die Vorgängerversion einer Datei oder eines Ordners aus Schattenkopien, die beim Anlegen eines Wiederherstellungspunkts erstellt werden, oder aus Sicherungssätzen wiederherstellen. Sie können eine umbenannte oder gelöschte Datei mit ihrem ursprünglichen Dateinamen wiederherstellen.

Rückblick auf dieses Kapitel

Sie können die in diesem Kapitel erworbenen Fähigkeiten folgendermaßen einüben und vertiefen:

- Lesen Sie die Zusammenfassung des Kapitels sorgfältig durch.
- Lesen Sie die Liste der Schlüsselbegriffe durch, die in diesem Kapitel eingeführt wurden.
- Arbeiten Sie die Übungen mit Fallbeispielen durch. Diese Szenarien beschreiben Fälle aus der Praxis, in denen die Themen dieses Kapitels zur Anwendung kommen. Sie werden aufgefordert, eine Lösung zu entwickeln.
- Führen Sie die vorgeschlagenen Übungen durch.
- Machen Sie einen Übungstest.

Schlüsselbegriffe

Wissen Sie, was die folgenden Schlüsselbegriffe bedeuten? Sie können Ihre Antworten überprüfen, indem Sie die Begriffe im Glossar am Ende des Buchs nachschlagen.

- **Dummywiederherstellung**
- **Wiederherstellungspunkt**
- **Schattenkopie**
- **Systemabbild**
- **Systemwiederherstellung**

Übungen mit Fallbeispiel

In den folgenden Übungen mit Fallbeispiel wenden Sie an, was Sie über Datensicherung und Wiederherstellung gelernt haben. Die Lösungen zu den Fragen finden Sie im Abschnitt »Antworten« hinten in diesem Buch.

Übung mit Fallbeispiel 1: Support für Datensicherung und Wiederherstellung

James Seymour ist ein IT-Experte, der bei einem großen Computerhändler arbeitet. Er berät Privatbenutzer, die beim Helpdesk des Unternehmens anrufen. Der Händler verkauft überwiegend Computer mit Windows 7.

Beantworten Sie die folgenden Fragen:

1. Ein Benutzer hat versehentlich alle Daten in einer Datei gelöscht, die Datei dann auf die Festplatte gespeichert und die Anwendung geschlossen. Er hat keine automatischen Datei- und Ordnersicherungen geplant. Er hat über eine Woche an der Datei gearbeitet. Während dieser Woche hat er mehrere Anwendungspakete installiert. Was sollte James ihm raten?
2. Eine Benutzerin hat die automatische Datei- und Ordnersicherung so konfiguriert, dass sie jeden Tag um Mitternacht durchgeführt wird. Sie hat die Standardeinstellung verwendet, sodass Windows auswählt, welche Dateien und Ordner gesichert werden. Eine Datei, an der ihr Sohn für ein Schulprojekt arbeitet, wurde beschädigt. Weil sie die Bibliothek *Dokumente* ihres Sohns nicht in der Datensicherung ausgewählt hat, macht sie sich Sorgen, dass sie die Datei nicht aus der Datensicherung wiederherstellen kann. Was sollte James ihr sagen?
3. Ein Benutzer hat vor Kurzem Software eines anderen Herstellers installiert, die auf seinem Computer Probleme verursacht. Es gelingt ihm auch nicht, diese Software zu deinstallieren. Er weiß, dass er mit der Systemwiederherstellung den Computer wieder auf den Stand des letzten Wiederherstellungspunkts zurücksetzen kann, aber er hat Angst, dass er dabei einige wichtige Dateien verliert, die er vor Kurzem erstellt hat. Was soll James ihm sagen?
4. Der Computer einer Kundin hat eine einzige Festplatte, die zwei Partitionen enthält. Die Kundin hat versucht, eine Systemabbildsicherung auf der Partition durchzuführen, die nicht das Betriebssystem enthält, aber der Assistent zum Erstellen eines Systemabbilds bietet diese Option nicht an. Sie will wissen, wie sie eine solche Datensicherung erstellen kann. Was soll James der Kundin raten?

Übung mit Fallbeispiel 2: Beseitigen von System- und Konfigurationsproblemen

James Seymour ist für den technischen Support bei Lucerne Publishing zuständig, einem kleinen Verlag, der nur eine Niederlassung hat. Das Netzwerk von Lucerne verwendet die Active Directory-Domänendienste nicht, sondern ist als Arbeitsgruppe konfiguriert. Alle Computer im Netzwerk laufen unter Windows 7 Professional. James hat auf allen Computern des Unternehmens ein Administratorkonto. Alle anderen Angestellten haben Standardkonten, die einzige Ausnahme ist der Chef, Don Hall, der für seinen eigenen Computer ein Adminis-

tratorkonto hat, aber nicht für die anderen. Leider hat Don nicht so viel Ahnung von Computern, wie er glaubt.

Beantworten Sie folgende Fragen:

1. Don startet seinen Computer neu und öffnet die erweiterten Startoptionen. Er wählt *Erzwingen der Treibersignatur deaktivieren* aus, damit er unsignierte Grafikkartentreiber installieren und ausprobieren kann, die er von verschiedenen Internetsites heruntergeladen hat. nachdem er allerdings den ersten dieser Treiber installiert hat, startet der Computer neu und zeigt einen völlig leeren Bildschirm. Don fragt James, wie er seinen Computer schnell wieder zum Laufen bekommt. Was soll James ihm raten?
2. Don denkt, er kennt eine bessere Methode, sein Problem zu lösen. Er will vom Installationsmedium starten und eine Systemabbildwiederherstellung ausführen. Glücklicherweise spricht er vorher mit James darüber. James weiß, dass die letzte Systemabbildsicherung, die auf Dons Computer durchgeführt wurde, 3 Monate zurückliegt. Was rät er Don?
3. Die Computer bei Lucerne Publishing haben zwei interne Festplatten. Die erste enthält das Betriebssystem und Anwendungen, die zweite Benutzerdaten. Datensicherungen werden in eine Netzwerkfreigabe auf einem Server geschrieben. Don sieht sich die Computerschutzeinstellungen an, die James auf der zweiten Festplatte konfiguriert hat. Er versteht, dass ein höherer Wert im Abschnitt *Maximale Belegung* bedeutet, dass mehr Vorgängerversionen gespeichert werden können. Er schlägt die Einstellung 90 Prozent vor statt der 40 Prozent, die James konfiguriert hat. Was sollte James ihm sagen?

Vorgeschlagene Übungen

Sie sollten die folgenden Aufgaben durcharbeiten, wenn Sie die in diesem Kapitel behandelten Prüfungsziele meistern wollen.

Durchführen von Datensicherungen

- **Übung 1** Schreiben Sie eine Batchdatei, die eine Systemabbildsicherung durchführt. Richten Sie in der Aufgabenplanung einen Zeitplan ein, sodass diese Datensicherung alle 2 Wochen ausgeführt wird.
- **Übung 2 (optional)** Wenn Sie einen zweiten Computer mit Windows 7 Ultimate in Ihrem Testnetzwerk haben (etwa den Computer *Aberdeen*), können Sie eine Netzwerkfreigabe auf diesem Computer anlegen und dann auf dem Computer *Canberra* eine Datei- und Ordnersicherung ausführen, die in diese Netzwerkfreigabe schreibt.

Konfigurieren der Systemwiederherstellung

- **Übung 1** Sie haben zwei Möglichkeiten, von der Installations-DVD zu starten und eine Systemwiederherstellung durchzuführen: Entweder Sie drücken beim Systemstart die Taste F8, um die erweiterten Startoptionen zu öffnen, oder Sie wählen *Computer reparieren* aus. Sie müssen wissen, wie Sie eine Systemwiederherstellung durchführen, wenn ein Computer nicht mehr normal startet.
- **Übung 2** Lesen Sie die Informationen zum Tool BCDEdit und seiner Befehlssyntax, auf die in Lektion 2 verwiesen wird. Üben Sie die Arbeit mit diesem Tool.

- **Übung 3 (optional)** Wenn Sie in Kapitel 2 eine startfähige VHD erstellt haben, können Sie eine neuere Systemabbildsicherung auf dieser VHD wiederherstellen und dann von diesem Systemabbild starten.

Wiederherstellen von Dateien und Ordnern

- **Übung 1** Löschen Sie eine Ihre Dateien (am besten eine, die Sie nicht mehr brauchen) und leeren Sie den Papierkorb. Stellen Sie die Datei wieder her und stellen Sie dabei sicher, dass die anderen Dateien im selben Ordner die neusten Versionen sind.
- **Übung 2** Löschen Sie all Ihre Internetfavoriten (kopieren Sie aber vorher Ihren Favoritenordner an einen sicheren Ort). Stellen Sie den Favoritenordner aus einer Benutzerprofilsicherung wieder her.

Machen Sie einen Übungstest

Die Übungstests (in englischer Sprache) auf der Begleit-CD zu diesem Buch bieten zahlreiche Möglichkeiten. Zum Beispiel können Sie einen Test machen, der ausschließlich die Themen aus einem Prüfungslernziel behandelt, oder Sie können sich selbst mit dem gesamten Inhalt der Prüfung 70-680 testen. Sie können den Test so konfigurieren, dass er dem Ablauf einer echten Prüfung entspricht, oder Sie können einen Lernmodus verwenden, in dem Sie sich nach dem Beantworten einer Frage jeweils sofort die richtige Antwort und Erklärungen ansehen können.



Weitere Informationen Übungstests

Einzelheiten zu allen Optionen, die bei den Übungstests zur Verfügung stehen, finden Sie im Abschnitt »So benutzen Sie die Übungstests« in der Einführung am Anfang dieses Buchs.

Antworten

Kapitel 1: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: C**
   A. **Falsch:** *LoadState.exe* gehört zum USMT (User State Migration Tool) und eignet sich nicht zur Vorbereitung eines USB-Speichergeräts als Windows 7-Installationsquelle.
   B. **Falsch:** *ScanState.exe* gehört zum USMT und eignet sich nicht zur Vorbereitung eines USB-Speichergeräts als Windows 7-Installationsquelle.
   C. **Richtig:** Mit dem Hilfsprogramm Diskpart können Sie ein USB-Speichergerät so vorbereiten, dass Sie den Computer von diesem Gerät starten können, um Windows 7 zu installieren.
   D. **Falsch:** BCDEdit dient zur Bearbeitung der Startkonfiguration und eignet sich nicht dafür, ein USB-Speichergerät so vorzubereiten, dass ein Computer von diesem Gerät gestartet und Windows 7 installiert werden kann.
2. **Richtige Antwort: D**
   A. **Falsch:** Sie müssen die Betriebssysteme in der Reihenfolge installieren, in der sie von Microsoft veröffentlicht wurden. Später erschienene Betriebssysteme sind in der Regel so ausgelegt, dass sie ältere Betriebssysteme erkennen, aber ältere Betriebssysteme können keine Installationen von Betriebssystemen erkennen, die nach ihnen erschienen sind.
   B. **Falsch:** Sie müssen die Betriebssysteme in der Reihenfolge installieren, in der sie erschienen sind. Später erschienene Betriebssysteme sind so ausgelegt, dass sie ältere Betriebssysteme erkennen, aber ältere Betriebssysteme können keine Installationen von Betriebssystemen erkennen, die nach ihnen erschienen sind.
   C. **Falsch:** Sie müssen die Betriebssysteme in der Reihenfolge installieren, in der sie erschienen sind. Später erschienene Betriebssysteme sind so ausgelegt, dass sie ältere Betriebssysteme erkennen, aber ältere Betriebssysteme können keine Installationen von Betriebssystemen erkennen, die nach ihnen erschienen sind.
   D. **Richtig:** Zuerst müssen Sie Windows XP installieren, dann Windows Vista und schließlich Windows 7, denn das ist die Reihenfolge, in der Microsoft die Betriebssysteme herausgebracht hat. Anschließend können Sie beim Start des Computers unter diesen drei Betriebssystemen wählen.
3. **Richtige Antworten: B und D**
   A. **Falsch:** Eine x86-Version von Windows 7 kann maximal 4 GByte Arbeitsspeicher verwenden.
   B. **Richtig:** Eine x64-Version von Windows 7 kann mehr als 4 GByte Arbeitsspeicher verwenden.

C. **Falsch:** Eine x86-Version von Windows 7 kann maximal 4 GByte Arbeitsspeicher verwenden.

D. **Richtig:** Eine x64-Version von Windows 7 kann mehr als 4 GByte Arbeitsspeicher verwenden.

4. **Richtige Antwort: B**

A. **Falsch:** Für eine Netzwerkinstallation mit WDS braucht ein Computer kein DVD-Laufwerk.

B. **Richtig:** Um ein Betriebssystem mit WDS über das Netzwerk hinweg bereitzustellen, muss der Computer mit einem WDS-Suchabbild gestartet werden oder über eine PXE-konforme Netzwerkkarte verfügen.

C. **Falsch:** Für eine Netzwerkinstallation mit WDS braucht ein Computer keinen USB 2.0-Anschluss.

D. **Falsch:** Für eine Netzwerkinstallation mit WDS braucht ein Computer keinen HDMI-Anschluss.

5. **Richtige Antwort: B**

A. **Falsch:** Für eine Dual-Boot-Konfiguration mit Windows XP und Windows 7 sind mindestens zwei Volumes erforderlich.

B. **Richtig:** Für eine Dual-Boot-Konfiguration mit Windows XP und Windows 7 sind mindestens zwei Volumes erforderlich. Das Windows 7-Installationsprogramm legt auf einem dieser Volumes ein zusätzliches 200-MByte-Systemvolume an, wenn Sie Windows 7 installieren, aber zwei Volumes ist die Mindestanzahl, die auf einem Windows XP-Computer zur Verfügung stehen muss, bevor Windows 7 in einer Dual-Boot-Konfiguration installiert wird.

C. **Falsch:** Für eine Dual-Boot-Konfiguration mit Windows XP und Windows 7 sind mindestens zwei Volumes erforderlich.

D. **Falsch:** Für eine Dual-Boot-Konfiguration mit Windows XP und Windows 7 sind mindestens zwei Volumes erforderlich.

Lektion 2

1. **Richtige Antwort: B**

A. **Falsch:** Sie können Windows Vista Enterprise nicht auf Windows 7 Home Professional aktualisieren. Windows Vista Enterprise (x86) kann nur auf Windows 7 Enterprise (x86) oder Ultimate (x86) aktualisiert werden.

B. **Richtig:** Windows Vista Enterprise (x86) kann nur auf Windows 7 Enterprise (x86) oder Ultimate (x86) aktualisiert werden.

C. **Falsch:** Sie können eine x86-Version von Windows Vista nicht auf eine x64-Version von Windows 7 aktualisieren.

D. **Falsch:** Sie können eine x86-Version von Windows Vista nicht auf eine x64-Version von Windows 7 aktualisieren.

2. **Richtige Antworten: A, B und D**

A. **Richtig:** Eine direkte Aktualisierung von Windows XP auf Windows 7 ist nicht möglich. Es bleibt also nur die Migration.

B. **Richtig:** Es ist nicht möglich, eine direkte Aktualisierung von einer x86-Version von Windows Vista auf eine x64-Version von Windows 7 durchzuführen.

C. **Falsch:** Sie können Windows Vista Enterprise (x64) direkt auf Windows 7 Enterprise (x64) aktualisieren.

D. **Richtig:** Es ist nicht möglich, eine direkte Aktualisierung von einer x64-Version von Windows Vista auf eine x86-Version von Windows 7 durchzuführen.

3. **Richtige Antwort: D**

A. **Falsch:** Sysprep eignet sich nicht zur Aktualisierung von einer Windows 7-Edition auf eine andere.

B. **Falsch:** Mit Windows PE können Sie keine Aktualisierungen von einer Windows 7-Edition auf eine andere durchführen.

C. **Falsch:** WDS setzt einen Server voraus, auf dem WDS installiert ist. Aus der Fragestellung geht hervor, dass in dem Heimnetzwerk kein anderer Computer verfügbar ist.

D. **Richtig:** Mit einer Internetverbindung kann ein Benutzer für die Aktualisierung von Windows 7 Home Premium auf Windows 7 Ultimate Windows Anytime Upgrade verwenden.

4. **Richtige Antwort: A**

A. **Richtig:** Der Windows 7 Upgrade Advisor kann die Konfiguration eines Windows Vista-Computers überprüfen und auf Anwendungen hinweisen, die auf dem Computer installiert sind und unter Windows 7 bekannte Kompatibilitätsprobleme aufweisen.

B. **Falsch:** Sysprep dient zur Vorbereitung eines Computers auf die Abbilderstellung. Das Programm gibt keine Auskunft über Kompatibilitätsprobleme mit Windows 7.

C. **Falsch:** Das USMT dient zur Migration von Benutzerprofildaten von einem Computer auf einen anderen. Es gibt keine Auskunft darüber, ob bestimmte Anwendungen Kompatibilitätsprobleme mit Windows 7 aufweisen.

D. **Falsch:** Windows PE ist ein einfaches Betriebssystem, das zur Installation von Windows Vista und Windows 7 und für Wartungsarbeiten verwendet wird. Es gibt keine Auskunft darüber, ob bestimmte Anwendungen Kompatibilitätsprobleme mit Windows 7 aufweisen.

5. **Richtige Antworten: A und C**

A. **Richtig:** Sie können einen Computer, auf dem Windows 7 Home Premium (x86) ausgeführt wird, auf Windows 7 Professional (x86) aktualisieren.

B. **Falsch:** Sie können eine x86-Version von Windows 7 nicht auf eine x64-Version von Windows 7 aktualisieren.

C. **Richtig:** Sie können einen Computer, auf dem Windows 7 Home Premium (x86) ausgeführt wird, auf Windows 7 Ultimate (x86) aktualisieren.

D. **Falsch:** Sie können eine x86-Version von Windows 7 nicht auf eine x64-Version von Windows 7 aktualisieren.

Lektion 3

1. **Richtige Antworten: B, C und D**
   A. **Falsch:** Windows 2000 unterstützt keine Offline-Migration mit USMT.
   B. **Richtig:** Windows XP Professional unterstützt die Offline-Migration mit USMT.
   C. **Richtig:** Windows Vista unterstützt die Offline-Migration mit USMT.
   D. **Richtig:** Windows 7 unterstützt die Offline-Migration mit USMT.
2. **Richtige Antworten: B und C**
   A. **Falsch:** Der Assistent zum Übertragen von Dateien und Einstellungen ist ein Programm von Windows XP. Es eignet sich nicht zur Übertragung von Daten auf Windows 7.
   B. **Richtig:** USMT kann für die Übertragung der Verschlüsselungszertifikate von Benutzern von einem Windows XP Professional-Computer auf einen Windows 7 Professional-Computer verwendet werden.
   C. **Richtig:** Windows-EasyTransfer kann für die Übertragung der Verschlüsselungszertifikate von Benutzern von einem Windows XP Professional-Computer auf einen Windows 7 Professional-Computer verwendet werden.
   D. **Falsch:** *RoboCopy.exe* kann nicht für die Übertragung der Verschlüsselungszertifikate von Benutzern von einem Windows XP Professional-Computer auf einen Windows 7 Professional-Computer verwendet werden.
3. **Richtige Antwort: B**
   A. **Falsch:** *MigDocs.xml* enthält Regeln über die Speicherorte der Dokumente der Benutzer.
   B. **Richtig:** *MigUser.xml* enthält Regeln für die Übertragung von Benutzerprofilen und Benutzerdaten.
   C. **Falsch:** *MigApp.xml* enthält Regeln für die Übertragung von Anwendungseinstellungen.
   D. **Falsch:** *Config.xml* enthält Informationen darüber, welche Elemente von einer Migration ausgeschlossen werden sollen.
4. **Richtige Antwort: C**
   A. **Falsch:** Windows Anytime Upgrade dient zur Aktualisierung einer Windows 7-Edition auf eine andere. Es enthält nicht USMT 4.0.
   B. **Falsch:** Windows Upgrade Advisor überprüft, ob die Hardware eines Windows Vista-Computers und die darauf installierte Software zu Windows 7 kompatibel ist.
   C. **Richtig:** Das WAIK enthält USMT 4.0.
   D. **Falsch:** Das Microsoft Application Compatibility Toolkit enthält nicht USMT 4.0.
5. **Richtige Antwort: C**
   A. **Falsch:** Unkomprimierte Migrationsspeicher beanspruchen am meisten Platz, weil in einer separaten Verzeichnisstruktur eine Kopie der zu übertragenden Daten erstellt wird.

B. **Falsch:** Komprimierte Migrationsspeicher enthalten eine komprimierte Kopie der zu übertragenden Daten in einer separaten Verzeichnisstruktur.

C. **Richtig:** Für Hard-link-Migrationsspeicher werden an einem separaten Ort feste Verknüpfungen mit den zu übertragenden Daten hergestellt, aber keine Kopien der Daten.

Kapitel 1: Antworten zu den Übungen mit Fallbeispiel

Übung 1: Installieren von Windows 7 bei Contoso

1. Sie könnten Windows 7 mit WDS oder einem USB-Speichergerät als Installationsquelle bereitstellen. Da Windows PE nicht in Frage kommt, können Sie keine Netzwerkfreigabe verwenden.
2. Sie könnten ein USB-Speichergerät als Installationsquelle für Windows 7 verwenden. Da Windows PE nicht in Frage kommt, können Sie keine Netzwerkfreigabe verwenden. Es lohnt sich nicht, an jedem Standort die Windows-Bereitstellungsdienste einzurichten, um Windows 7 auf 5 Computern zu installieren.
3. Windows 7 Enterprise unterstützt die BitLocker-Laufwerkverschlüsselung und ist für Volumenlizenzkunden verfügbar. Windows 7 Ultimate unterstützt zwar ebenfalls die BitLocker-Laufwerkverschlüsselung, wird aber mit Einzellizenzen und nicht mit Volumenlizenzen vertrieben.

Übung 2: Migrieren von Benutzerdaten bei Fabrikam

1. Side-by-Side-Migrationen bieten sich an, weil die Benutzer in der Zweigstelle von alten auf neue Computer wechseln. Wipe-and-Load-Migrationen sind nur sinnvoll, wenn dieselbe Computerhardware weiterverwendet werden soll.
2. In der Zentrale führen Sie Wipe-and-Load-Migrationen durch, weil die Benutzer in der Zentrale dieselbe Computerhardware weiterverwenden, aber die x86-Version von Windows 7 Enterprise nach der Aktualisierung nicht mehr verwenden sollen.
3. Verwenden Sie Windows-EasyTransfer mit der Übertragung über das Netzwerk.

Kapitel 2: Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: D**

   A. **Falsch:** Wenn Sie ein Windows 7-WIM-Abbild aufzeichnen wollen, müssen Sie den Computer unter Windows PE 3.0 (Windows PE) starten.

   B. **Falsch:** Wenn Sie ein Windows 7-WIM-Abbild aufzeichnen wollen, müssen Sie den Computer unter Windows PE 3.0 (Windows PE) starten. Außerdem dient das Tool Windows SIM dazu, Windows-Abbilder zu öffnen, Antwortdateien zu erstellen und Bereitstellungsfreigaben und Konfigurationssätze zu verwalten. Es erstellt keine WIM-Abbilder.

   C. **Falsch:** Wenn Sie ein Windows 7-WIM-Abbild aufzeichnen wollen, müssen Sie den Computer unter Windows PE 3.0 (Windows PE) starten. Außerdem dient das

Tool DISM dazu, Updates, Treiber und Language Packs auf ein Windows-Abbild anzuwenden. Es erstellt keine WIM-Abbilder.

D. **Richtig:** Um ein Windows 7-WIM-Abbild aufzuzeichnen, starten Sie den Computer unter Windows PE 3.0 (Windows PE) und benutzen das Tool ImageX.

E. **Falsch:** Das Tool Windows SIM dient dazu, Windows-Abbilder zu öffnen, Antwortdateien zu erstellen und Bereitstellungsfreigaben und Konfigurationssätze zu verwalten. Es erstellt keine WIM-Abbilder.

F. **Falsch:** Das Tool DISM dient dazu, Updates, Treiber und Language Packs auf ein Windows-Abbild anzuwenden. Es erstellt keine WIM-Abbilder.

2. **Richtige Antworten: A und E**

A. **Richtig:** Das Tool Windows SIM aus dem Windows AIK automatisiert die Erstellung einer Antwortdatei für die unbeaufsichtigte Installation. Im Fensterabschnitt *Antwortdatei* von Windows SIM können Sie unter *Einstellungen* die gewünschten Einstellungen auswählen und die jeweiligen Werte in der rechten Spalte eingeben.

B. **Falsch:** DISM wendet Updates, Treiber und Language Packs auf ein Windows-Abbild an. Sie können damit keine Antwortdatei erstellen.

C. **Falsch:** Mit der Deployment Workbench können Sie auf die MDT 2010-Dokumentation zugreifen, Tasksequenzen erstellen und konfigurieren, Bereitstellungspunkte auflisten und eine Bereitstellungsfreigabe anlegen. Eine Antwortdatei können Sie damit nicht erstellen.

D. **Falsch:** *Sysprep.exe* bereitet einen Computer für die Abbildbereitstellung vor. Sie können eine Antwortdatei verwenden, um den Sysprep-Prozess zu automatisieren, aber es ist nicht möglich, mit *Sysprep.exe* eine Antwortdatei zu erstellen.

E. **Richtig:** Windows SIM automatisiert zwar den Prozess, aber manche erfahrene Administratoren schreiben ihre Antwortdatei für die unbeaufsichtigte Installation lieber direkt in einem Texteditor wie dem Windows-Editor.

3. **Richtige Antworten: A, C, F, G und H**

A. **Richtig:** Sie brauchen das Tool ImageX und die Windows PE-Tools, um ein Systemabbild auf dem Referenzcomputer zu erstellen. Außerdem brauchen Sie das Tool Oscdimg, um eine ISO-Datei zu generieren und ein startfähiges Windows PE-Medium zu erstellen. Daher müssen Sie das Windows AIK installieren.

B. **Falsch:** Es ist nicht unbedingt nötig, zum Konfigurieren des Referenzcomputers eine Antwortdatei zu verwenden, auch wenn Microsoft diese Methode empfiehlt. Wenn es Ihnen lieber ist, können Sie den Computer auch von Hand konfigurieren.

C. **Richtig:** Sie müssen ein Betriebssystem auf Ihrem Referenzcomputer installieren, damit Sie ein Abbild davon aufzeichnen können.

D. **Falsch:** Die Aufgabe gibt nicht vor, wie das Abbild verteilt wird. MDT ist nur eine von mehreren Möglichkeiten. Wenn Sie MDT einsetzen und das Abbild auf sehr vielen Zielcomputern bereitstellen, werden Sie es wahrscheinlich auf einem Server installieren.

E. **Falsch:** Die Aufgabe gibt nicht vor, wie das Abbild verteilt wird. WDS ist nur eine von mehreren Möglichkeiten. Es ist in der Aufgabe auch nicht angegeben, ob die Zielcomputer PXE-kompatibel sind.

F. **Richtig:** Sie müssen den Referenzcomputer unter Windows PE starten, um sein Abbild aufzuzeichnen.

G. **Richtig:** Ihr Ziel besteht darin, ein Abbild des Referenzcomputers zu erstellen. Dafür verwenden Sie das Tool ImageX.

H. **Richtig:** Sie verteilen das Abbild auf mehrere Computer. Daher müssen Sie den Referenzcomputer mit `sysprep /generalize` und `sysprep /oobe` auf die Abbilderstellung vorbereiten.

4. **Richtige Antwort: C**

   A. **Falsch:** Der Befehl `sysprep /audit` startet den Computer im Überwachungsmodus. Hier können Sie Treiber oder Anwendungen zu Windows 7 hinzufügen und die Installation testen, bevor sie an einen Benutzer gesendet wird. Der Befehl entfernt keine eindeutigen Systeminformationen aus der Installation.

   B. **Falsch:** Der Befehl `sysprep /oobe` startet den Computer mit der Windows-Willkommensseite. Hier können Benutzer ihr Windows 7 anpassen, Benutzerkonten anlegen und dem Computer einen Namen geben. Der Befehl entfernt keine eindeutigen Systeminformationen aus der Installation.

   C. **Richtig:** Der Befehl `sysprep /generalize` entfernt alle eindeutigen Systeminformationen aus der Windows 7-Installation. Die SID wird zurückgesetzt, Systemwiederherstellungspunkte werden entfernt und Ereignisprotokolle werden gelöscht.

   D. **Falsch:** Der Befehl `sysprep /unattend`, gefolgt vom Namen einer Antwortdatei, wendet während einer unbeaufsichtigten Installation die Einstellungen aus der Antwortdatei auf Windows 7 an. Der Befehl entfernt keine eindeutigen Systeminformationen aus der Installation.

5. **Richtige Antwort: A**

   A. **Richtig:** Der Konfigurationsdurchlauf *oobeSystem* des Windows-Setups wendet Einstellungen auf Windows 7 an, bevor die Windows-Willkommensseite startet.

   B. **Falsch:** Der Konfigurationsdurchlauf *auditSystem* des Windows-Setups verarbeitet Einstellungen für die unbeaufsichtigte Installation, während Windows 7 im Systemkontext läuft und noch bevor sich ein Benutzer im Überwachungsmodus am Computer anmeldet. Er wendet keine Einstellungen auf Windows 7 an, bevor die Windows-Willkommensseite startet.

   C. **Falsch:** Der Konfigurationsdurchlauf *specialize* des Windows-Setups erstellt systemspezifische Informationen wie Netzwerkeinstellungen, internationale Einstellungen und Domäneninformationen und wendet sie an. Er wendet keine Einstellungen auf Windows 7 an, bevor die Windows-Willkommensseite startet.

   D. **Falsch:** Der Konfigurationsdurchlauf *offlineServicing* des Windows-Setups wendet Updates auf ein Windows-Abbild an. Außerdem wendet er Pakete an, beispielsweise Softwarefixes, Language Packs und andere Sicherheitsupdates. Während dieses Durchlaufs können Sie Treiber zu einem Windows 7-Abbild hinzufügen, bevor das Abbild installiert wird. Dieser Durchlauf wendet keine Einstellungen auf Windows 7 an, bevor die Windows-Willkommensseite startet.

Lektion 2

1. **Richtige Antwort: B**
   A. **Falsch:** Eine VHD wird als Datei mit der Erweiterung *.vhd* erstellt. Sie müssen den Dateinamen *Systemvhd.vhd* angeben.
   B. **Richtig:** Damit wird die angegebene VHD-Datei erstellt.
   C. **Falsch:** Die Größe (oder Maximalgröße) der VHD wird in der Einheit MByte angegeben, nicht in GByte. Daher muss der Wert 20000 lauten, nicht 20.
   D. **Falsch:** Eine VHD wird als Datei mit der Erweiterung *.vhd* erstellt. Sie müssen den Dateinamen *Systemvhd.vhd* angeben. Außerdem wird die Größe (oder Maximalgröße) der VHD in der Einheit MByte angegeben, nicht in GByte. Daher muss der Wert 20000 lauten, nicht 20.
2. **Richtige Antwort: C**
   A. **Falsch:** Dieser Befehl zwingt Windows 7, die HAL beim Erstellen des Starteintrags automatisch zu erkennen.
   B. **Falsch:** Dieser Befehl löscht einen VHD-Eintrag aus dem Systemstartmenü.
   C. **Richtig:** Dieser Befehl prüft, ob der Starteintrag richtig erstellt wurde.
   D. **Falsch:** Dieser Befehl gibt die GUID der angegebenen VHD zurück.
3. **Richtige Antwort: D**
   A. **Falsch:** Dieser Befehl ersetzt ein Installationsabbild. Üblicherweise verwenden Sie diesen Befehl, wenn Sie ein Installationsabbild aktualisiert haben und die alte Abbilddatei überschreiben wollen.
   B. **Falsch:** Dieser Befehl aktiviert auf dem WDS-Server die Richtlinie zum automatischen Hinzufügen.
   C. **Falsch:** Dieser Befehl erstellt ein Suchabbild.
   D. **Richtig:** Dieser Befehl fügt ein Installationsabbild hinzu, wie in der Aufgabe gefordert.
4. **Richtige Antwort: A**
   A. **Richtig:** Das Offline Virtual Machine Servicing Tool arbeitet mit SCVMM zusammen. Seine wichtigste Aufgabe besteht darin, eine geplante Aufgabe anzulegen und auszuführen, die VHDs und virtuelle Computer gerade so lange online bringt, dass sie Updates für ihre Systemabbilder herunterladen können, gewöhnlich von einem WSUS-Server.
   B. **Falsch:** SCVMM ist eine Voraussetzung, damit das Offline Virtual Machine Servicing Tool installiert und ausgeführt werden kann. Aber dieses Tool implementiert die regelmäßigen Systemstarts von VHDs, die normalerweise offline sind.
   C. **Falsch:** Das MMC-Snap-In *Windows-Bereitstellungsdienste* ist ein GUI-Tool, das zur Verfügung steht, wenn Sie die WDS-Serverrolle installieren. Sie können darin Datenträgerabbilder erstellen, bearbeiten und exportieren. Es bietet allerdings keine Möglichkeit, regelmäßige Systemstarts von VHDs auszuführen, die normalerweise offline sind.

D. **Falsch:** WDSUTIL ist ein Befehlszeilentool, das zur Verfügung steht, wenn Sie die WDS-Serverrolle installieren. Sie können damit Datenträgerabbilder erstellen, bearbeiten und exportieren oder Clientcomputer vorab bereitstellen. Es bietet allerdings keine Möglichkeit, regelmäßige Systemstarts von VHDs auszuführen, die normalerweise offline sind.

Kapitel 2: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Generieren eines Systemabbilds

1. Sie sollten eine WIM-Abbilddatei generieren. Dazu verwenden Sie das Tool ImageX aus dem Windows AIK.
2. Sie sollten eine ISO-Abbilddatei generieren. Dazu verwenden Sie das Tool Oscdimg aus dem Windows AIK.
3. Mit USMT aus dem Windows AIK können Sie Benutzerdaten von Computern, die unter Windows Vista Ultimate laufen, auf Windows 7 Ultimate-Computer übertragen.

Übung mit Fallbeispiel 2: Arbeiten mit VHDs

1. Sie können nur den Windows 7 Ultimate-Computer unter dem Betriebssystem starten, das in seiner VHD aufgezeichnet wurde. Nur Windows 7 Enterprise und Windows 7 Ultimate bieten die Möglichkeit, ein System zu starten, das auf einer VHD installiert ist.
2. Sie müssen `sysprep /generalize` ausführen, um hardwarespezifische Informationen wie die SID aus dem Abbild zu entfernen, das aus dem Referenzcomputer generiert wird.

Kapitel 3: Lernzielkontrolle

Lektion 1

1. **Richtige Antworten: B und D**
   A. **Falsch:** Das DISM-Argument `/image` gibt an, welcher Ordner das bereitgestellte Abbild enthält, nicht das Quellabbild.
   B. **Richtig:** Das Argument `/recurse` gibt an, dass alle Treiber aus dem Ordner *C:\Drivers* und allen seinen Unterordnern zum bereitgestellten Abbild hinzugefügt werden.
   C. **Falsch:** Das DISM-Argument `/image` gibt an, welcher Ordner das bereitgestellte Abbild enthält, nicht das Quellabbild.
   D. **Richtig:** Dieser Befehl funktioniert, allerdings ist Antwort B die bessere Lösung. Üblicherweise geben Sie `/driver` nur dann mehrmals an, wenn die Treiber nicht in derselben Dateistruktur liegen (zum Beispiel in *C:\Printerdriver* und *C:\Scannerdriver*).
2. **Richtige Antwort: A**
   A. **Richtig:** Der beschreibbare Speicher, der in einem Windows PE-Systemvolume zur Verfügung steht, sobald es im RAM-Disk-Modus gestartet wurde, wird als Entwurfsspeicher (scratch space) des Windows PE-Systemvolumes bezeichnet. Mit dem DISM-Argument `/get-scratchspace` legen Sie dessen Größe fest.

B. **Falsch:** Dieser Befehl gibt den Pfad zum Stammverzeichnis des Windows PE-Abbilds beim Systemstart zurück, den sogenannten Zielpfad.

C. **Falsch:** Dieser Befehl ermittelt, ob das Windows PE-Profilerstellungstool aktiviert oder deaktiviert ist.

D. **Falsch:** Die Profilerstellung (Dateiprotokollierung) ist in der Standardeinstellung deaktiviert. Dieser Befehl aktiviert sie. Der Befehl meldet aber nicht, wie viel beschreibbarer Speicher in einem Windows PE-Systemvolume zur Verfügung steht, sobald es im RAM-Disk-Modus gestartet wird.

3. **Richtige Antwort: D**

A. **Falsch:** Das Argument `/set-syslocale` legt die Sprache für Nicht-Unicode-Programme (das sogenannte Systemgebietsschema) und die Schriftarteinstellungen fest. Dies ist nur bei einem offline bereitgestellten Abbild möglich.

B. **Falsch:** Das Argument `/set-userlocale` konfiguriert eine benutzerspezifische Einstellung, mit der die Standardsortierreihenfolge und die Standardeinstellungen für die Formatierung von Datum, Uhrzeit, Währung und Zahlen festgelegt werden. Dies ist nur bei einem offline bereitgestellten Abbild möglich.

C. **Falsch:** Das Argument `/set-inputlocale` legt das Eingabegebietsschema und das Tastaturlayout fest. Dies ist nur bei einem offline bereitgestellten Abbild möglich.

D. **Richtig:** Bei einem laufenden Onlinebetriebssystem können Sie die internationalen Einstellungen abfragen, sie aber nicht konfigurieren. Das DISM-Argument `/get-intl` ist das einzige, das Sie bei einem Onlineabbild verwenden dürfen.

4. **Richtige Antwort: B**

A. **Falsch:** Das bereitgestellte Abbild liegt in *C:\Mount*, nicht in *C:\Textfiles\Answer*. Die Antwortdatei liegt in *C:\Textfiles\Answer*, nicht in *C:\Mount*.

B. **Richtig:** Dieser Befehl wendet die Datei *Unattend.xml* aus dem Ordner *C:\Textfiles\Answer* auf ein Abbild an, das im Ordner *C:\Mount* bereitgestellt wurde.

C. **Falsch:** Das DISM-Argument, das eine Antwortdatei auf ein bereitgestelltes Abbild anwendet, ist `/apply-unattend`, nicht `/apply`.

D. **Falsch:** Das DISM-Argument, das eine Antwortdatei auf ein bereitgestelltes Abbild anwendet, ist `/apply-unattend`, nicht `/apply-answer`.

5. **Richtige Antwort: C**

A. **Falsch:** Das DISM-Argument `/get-appinfo` liefert Informationen über Windows Installer-Anwendungen (*.msi*). Das Argument `/get-packageinfo` liefert dagegen Informationen über Pakete, die in Form von *.cab*-Dateien vorliegen.

B. **Falsch:** Das DISM-Argument `/get-appinfo` liefert Informationen über Windows Installer-Anwendungen (*.msi*). Das Argument `/get-featureinfo` liefert dagegen Informationen über Windows-Features.

C. **Richtig:** Das DISM-Argument `/get-appinfo` liefert Informationen über Windows Installer-Anwendungen (*.msi*).

D. **Falsch:** Das DISM-Argument `/get-appinfo` liefert Informationen über Windows Installer-Anwendungen (*.msi*). Das Argument `/get-apppatchinfo` liefert dagegen Informationen über Anwendungspatches (*.msp*-Dateien).

Lektion 2

1. **Richtige Antwort: B**
   A. **Falsch:** MDT 2010 kann Updates, Anwendungen und Language Packs zu einem WIM-Systemabbild hinzufügen, das dann auf Clientcomputern und VHDs installiert wird. Es ist aber nicht in der Lage, VHDs direkt zu aktualisieren.
   B. **Richtig:** Mit dem Offline Virtual Machine Servicing Tool können Sie VHD-Offlinedateien, die Installationen von Windows 7 enthalten, mit Service Packs und Softwareupdates auf dem neusten Stand halten.
   C. **Falsch:** Sie können das Befehlszeilentool BCDEdit verwenden, um einen Starteintrag für eine VHD hinzuzufügen. Das Tool aktualisiert aber keine VHDs.
   D. **Falsch:** Sie können das Offline Virtual Machine Servicing Tool mit VMM 2007 und WSUS 3.0, SCCM 2007 oder Configuration Manager 2007 R2 verwenden. Configuration Manager 2007 R2 ist aber nicht in der Lage, VHDs direkt zu aktualisieren.
2. **Richtige Antwort: D**
   A. **Falsch:** Wenn Sie einen Referenzcomputer von einem WDS-Aufzeichnungsabbild starten, können Sie mit dem Assistenten zur Abbildaufzeichnung der Windows-Bereitstellungsdienste ein Systemabbild dieses Computers aufzeichnen und es auf den WDS-Server exportieren. Dabei wird nicht direkt angegeben, in welchem Quellverzeichnis die WIM-Datei liegt, nicht ausgewählt, ob Setup- oder Sysprep-Dateien benötigt werden, und die Datei nicht in die Bereitstellungsfreigabe verschoben.
   B. **Falsch:** Der Tasksequenz-Editor von SCCM 2007 erstellt und bearbeitet Tasksequenzen. Im Tasksequenzerstellungs-Assistenten haben Sie die Wahl zwischen *Bestehendes Abbildpaket installieren*, *Referenz-Betriebssystemabbild erstellen* und *Neue benutzerdefinierte Tasksequenz erstellen*. Der Assistent erstellt aber nur Tasksequenzen. Es wird dabei nicht direkt angegeben, in welchem Quellverzeichnis die WIM-Datei liegt, nicht ausgewählt, ob Setup- oder Sysprep-Dateien benötigt werden, und die Datei nicht in die Bereitstellungsfreigabe verschoben.
   C. **Falsch:** Sie starten den Assistenten für neue Bereitstellungsfreigaben (*New Deployment Share Wizard*) in der Konsole *Deployment Workbench* von MDT 2010. In diesem Assistenten legen Sie eine Bereitstellungsfreigabe an, in der die WIM-Datei abgelegt wird. Aber es wird dabei nicht direkt angegeben, in welchem Quellverzeichnis die WIM-Datei liegt, nicht ausgewählt, ob Setup- oder Sysprep-Dateien benötigt werden, und die Datei nicht in die Bereitstellungsfreigabe verschoben.
   D. **Richtig:** Sie starten den Assistenten zum Importieren von Betriebssystemen (*Import Operating System Wizard*) in der Konsole *Deployment Workbench* von MDT 2010. In diesem Assistenten geben Sie an, in welchem Quellverzeichnis die WIM-Datei liegt, wählen aus, ob Setup- oder Sysprep-Dateien benötigt werden, und verschieben die Datei in die Bereitstellungsfreigabe.

3. **Richtige Antwort: C**
   A. **Falsch:** WDS stellt Installationsabbilder über das Netzwerk bereit. Sie brauchen sie nicht auf einem startfähigen Wechseldatenträger zu installieren.
   B. **Falsch:** Wenn Sie einen Zielcomputer aus dem Netzwerk starten, zeigt WDS ein Systemstartmenü auf dem Zielcomputer an, in dem Sie ein Startabbild auswählen, das gestartet wird. Dieses Abbild wird über das Netzwerk übertragen, daher brauchen Sie es nicht auf einem startfähigen Wechseldatenträger zu installieren. Beachten Sie, dass ein Standardstartabbild zur Auswahl angeboten wird. Such- und Aufzeichnungsabbilder sind spezielle Typen von Startabbildern.
   C. **Richtig:** Falls Ihre Zielcomputer nicht PXE-kompatibel sind, können sie nicht über das Netzwerk starten. Daher müssen Sie sie von einem Suchabbild starten, das auf einem startfähigen Wechseldatenträger gespeichert ist.
   D. **Falsch:** Wenn Sie das Abbild eines Referenzcomputers aufzeichnen, starten Sie ihn von einem Aufzeichnungsabbild. Aufzeichnungsabbilder werden im Systemstartmenü genauso wie Standardstartabbilder aufgelistet, Sie brauchen sie daher nicht auf einem startfähigen Wechseldatenträger zu installieren.
4. **Richtige Antworten: A, E und F**
   A. **Richtig:** Die WDS-Serverrolle muss auf einem Server in einer AD DS-Domäne installiert sein.
   B. **Falsch:** WDS kann mit MDT 2010 zusammenarbeiten, um LTI zu implementieren. MDT 2010 ist aber nicht unbedingt nötig, um Abbilder bereitzustellen.
   C. **Falsch:** SQL Server wird neben SCCM 2007 und MDT 2010 gebraucht, um ZTI zu implementieren. SQL Server wird aber nicht für WDS vorausgesetzt.
   D. **Falsch:** SCCM 2007 wird neben SQL Server und MDT 2010 gebraucht, um ZTI zu implementieren. SCCM 2007 wird aber nicht für WDS vorausgesetzt.
   E. **Richtig:** WDS stellt Abbilder normalerweise auf PXE-kompatiblen Zielcomputern bereit, die DHCP für ihre IP-Konfiguration brauchen.
   F. **Richtig:** Die WDS-Serverrolle muss auf einem Server in einem Netzwerk installiert werden, das mindestens einen DNS-Server enthält.
5. **Richtige Antwort: A**
   A. **Richtig:** Um das Abbild startfähig zu machen, verwenden Sie BCDboot aus Windows PE. Damit initialisieren Sie den BCD-Speicher und kopieren Startumgebungsdateien in die Systempartition. Beim Neustart startet der Zielcomputer unter Windows 7 Ultimate.
   B. **Falsch:** Mit DISM können Sie ein WIM-Abbild verwalten und bearbeiten. Es macht ein Abbild nicht startfähig, wenn Sie es auf einem Zielcomputer installiert haben.
   C. **Falsch:** Mit BCDEdit machen Sie Medien wie VHDs und USB-Flashsticks startfähig. Es macht kein Abbild startfähig, das Sie auf einem Zielcomputer installiert haben.
   D. **Falsch:** Sie verwenden ImageX, um das WIM-Abbild auf dem Quellcomputer zu erstellen und es auf dem Zielcomputer zu installieren. ImageX ist aber nicht in der Lage, das installierte Abbild startfähig zu machen.

Kapitel 3: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Bereitstellen eines Abbilds mit mehreren Language Packs

1. Don braucht:
   - Einen Administrationscomputer, auf dem die Windows AIK-Tools installiert sind und auf dessen Festplattenlaufwerk genug Platz frei ist, um das Masterabbild zu speichern und es im Dateisystem bereitzustellen.
   - Das Windows-Abbild (*.wim*-Datei), das er bearbeiten will.
   - Die Treiber (*.inf*-Dateien), Updatepakete (*.cab*- oder *.msu*-Dateien) und Language Packs (*.cab*-Dateien), die er bei der Wartung des Abbilds verwendet.
2. Dons erste Aufgabe besteht darin, eine Instanz des Masterabbilds auf den Administrationscomputer zu kopieren. Microsoft rät davon ab, ein Abbild aus einer Netzwerkfreigabe im Dateisystem bereitzustellen.
3. Don verwendet DISM, um das Abbild im Dateisystem bereitzustellen. Dann führt er DISM-Befehle aus, um das Update anzuwenden, den neuen Treiber hinzuzufügen und die gewünschten Einstellungen zu ändern. Er prüft, ob beide Language Packs im Abbild installiert sind und ob die richtigen internationalen Einstellungen konfiguriert werden können. Sofern abzusehen ist, dass er das Abbild regelmäßig pflegen muss, sollte er ein Skript schreiben, das die erforderlichen DISM-Befehle aufruft. Don verwendet DISM außerdem, um sicherzustellen, dass die richtigen Treiber und andere Pakete zum Abbild hinzugefügt (oder eventuell daraus entfernt) wurden. Und schließlich verwendet er DISM, um die Änderungen in das Abbild zu übernehmen und seine Bereitstellung im Dateisystem aufzuheben.

Übung mit Fallbeispiel 2: Bereitstellen eines Abbilds auf 100 Clientcomputern

1. Sie müssen sicherstellen, dass alle kritischen und empfohlenen Updates eingespielt wurden, vor allem die Sicherheitsupdates. Werden neue Hardwaregeräte mit den Computern benutzt, die nicht Plug & Play-fähig sind, müssen Sie die entsprechenden Gerätetreiber auf dem Referenzcomputer installieren. Sie müssen die Installation sorgfältig testen. Und schließlich müssen Sie die Computerkonfiguration mit dem Tool Sysprep verallgemeinern, bevor Sie das Abbild aufzeichnen.
2. Sie müssen ein Aufzeichnungsabbild auf dem WDS-Server erstellen.
3. Starten Sie den Referenzcomputer neu und drücken Sie F12, um aus dem Netzwerk zu starten. Wählen Sie im Systemstartmenü das Aufzeichnungsabbild aus und führen Sie die Schritte zum Erstellen eines Systemabbilds durch. Übertragen Sie die fertige WIM-Datei auf den WDS-Server. Starten Sie jeden Zielcomputer aus dem Netzwerk (bei Bedarf müssen Sie dazu die Startreihenfolge im BIOS ändern). Wählen Sie im Systemstartmenü das Standardstartabbild (nicht das Aufzeichnungsabbild) aus und verwenden Sie das Installationsabbild, das Sie auf dem Referenzcomputer aufgezeichnet haben. Dieses Abbild wird nun installiert und das Setup wird normal fortgesetzt.

Kapitel 4: Lernzielkontrolle

Lektion 1

1. **Richtige Antworten: A und C**
   A. **Richtig:** Der Gerätetreiber muss mit einem gültigen digitalen Zertifikat signiert sein, das von Windows 7 akzeptiert wird und im Speicher *Vertrauenswürdige Herausgeber* eingetragen ist. Andernfalls werden Administratorprivilegien gebraucht, um das Gerät zu installieren.
   B. **Falsch:** Im Speicher *Vertrauenswürdige Herausgeber* sind digitale Zertifikate gespeichert, keine Gerätetreiber.
   C. **Richtig:** Der Gerätetreiber muss im Gerätetreiberspeicher vorliegen. Andernfalls werden Administratorprivilegien gebraucht, um den Treiber in diesen Speicher zu kopieren.
   D. **Falsch:** Das Gerät braucht nicht über einen USB-Anschluss mit dem Computer verbunden zu sein. Es kann unter anderem auch eine PS/2-Tastatur sein.
   E. **Falsch:** Microsoft signiert zwar viele Treiber, aber eine Signatur von Microsoft ist nicht zwingend notwendig. Das digitale Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt sein. In der Domänenumgebung kann es sich beispielsweise um ein selbstsigniertes Zertifikat handeln.
2. **Richtige Antwort: B**
   A. **Falsch:** Auf diese Weise stellen Sie fest, wie viel Strom jedes Gerät braucht, nicht die Bandbreitenanforderungen.
   B. **Richtig:** In der Liste *Geräte, die Bandbreite verwenden* auf der Registerkarte *Erweitert* erfahren Sie die Bandbreitenanforderungen für jedes Gerät.
   C. **Falsch:** Die Registerkarte *Details* enthält viele Informationen (etwa die GUID für den Gerätetyp), gibt aber nicht über die Bandbreitenanforderungen Auskunft. Außerdem sind die hier aufgeführten Geräte nicht unbedingt an den USB-Hub angeschlossen.
   D. **Falsch:** IEEE-1394-Bus-Hostcontroller sind keine USB-Geräte. Außerdem zeigt die Registerkarte *Ressourcen* keine Bandbreitenanforderungen an.
3. **Richtige Antworten: A und D**
   A. **Richtig:** So können Nicht-Administratoren alle Geräte aus der angegebenen Gerätesetupklasse installieren, sofern der Gerätetreiber sich im Treiberspeicher befindet.
   B. **Falsch:** Damit weisen Sie Windows 7 an, in allen Ordnern und Unterordnern von Laufwerk *C:* nach einem Gerätetreiber zu suchen. Es werden aber Administratorprivilegien gebraucht, um den Treiber in den Treiberspeicher zu kopieren und ihn zu installieren.
   C. **Falsch**: Der Speicher *Vertrauenswürdige Herausgeber* enthält digitale Zertifikate, die Treibersignaturen authentifizieren. Er speichert keine Gerätetreiber.
   D. **Richtig:** Wird ein Treiber bereitgestellt, wird er in den Gerätetreiberspeicher kopiert. Nicht-Administratoren können dann das Gerät installieren, sofern sie die Berechtigung haben, Geräte der jeweiligen Gerätesetupklasse zu installieren.

4. **Richtige Antwort: B**
   A. **Falsch:** So wird verhindert, dass Treiber, die aus Windows Update heruntergeladen wurden, automatisch installiert werden. Sie entfernen die Website damit aber nicht aus dem Suchpfad.
   B. **Richtig:** So verhindern Sie, dass Windows 7 in Windows Update nach Gerätetreibern sucht.
   C. **Falsch:** Der Registrierungseintrag *DevicePath* führt die Windows Update-Website nicht auf.
   D. **Falsch:** Bei dieser Einstellung werden Treiber aus Windows Update installiert, wenn Windows 7 anhand bestimmter Kriterien berechnet, dass sie sich am besten eignen. Sie verhindern damit aber nicht, dass Windows 7 in Windows Update nach Gerätetreibern sucht.
5. **Richtige Antwort: A**
   A. **Richtig:** Damit beenden Sie den Gerätetreiber, wodurch das Gerät sofort deaktiviert wird.
   B. **Falsch:** So stellen Sie sicher, dass das Gerät deaktiviert ist, wenn der Computer das nächste Mal gestartet wird. Das ist sinnvoll, wenn Sie feststellen, dass das Gerät Probleme verursacht. Das Gerät wird dabei aber nicht sofort beendet, sodass Sie das Problem untersuchen können.
   C. **Falsch:** Die Schaltfläche *Deaktivieren* steht bei PnP-Geräten zur Verfügung, aber nicht bei Geräten, die unter *Nicht-PnP-Treiber* aufgeführt sind. Verwenden Sie stattdessen die Schaltfläche *Beenden*.
   D. **Falsch:** Die Schaltfläche *Deinstallieren* steht bei PnP-Geräten zur Verfügung, aber nicht bei Geräten, die unter *Nicht-PnP-Treiber* aufgeführt sind. Ohnehin wollen Sie den Treiber beenden, nicht deinstallieren.

Lektion 2

1. **Richtige Antwort: A**
   A. **Richtig:** Dieser Diskpart-Befehl konvertiert den ausgewählten Datenträger in einen GPT-Datenträger.
   B. **Falsch:** Dieser Diskpart-Befehl konvertiert den ausgewählten Datenträger in einen MBR-Datenträger.
   C. **Falsch:** Dieser Diskpart-Befehl konvertiert den ausgewählten dynamischen Datenträger in einen Basisdatenträger.
   D. **Falsch:** Dieser Diskpart-Befehl konvertiert den ausgewählten Basisdatenträger in einen dynamischen Datenträger.
2. **Richtige Antwort: C**
   A. **Falsch:** Das ist eine sinnvolle Strategie bei Windows 7 Enterprise oder Ultimate Edition, aber auf einem Computer mit Windows 7 Home Premium können Sie eine VHD nicht startfähig machen.
   B. **Falsch:** RAID-0 (Stripset) bietet keine Fehlertoleranz, und Sie können Betriebssystemdateien nicht auf einem RAID-0-Volume ablegen.

C. **Richtig:** Mit einem RAID-1-Volume erstellen Sie einen Spiegel der Festplatte, die Ihr Betriebssystem enthält. So erreichen Sie Fehlertoleranz.

D. **Falsch:** RAID-5 bietet Fehlertoleranz und Ausfallschutz. Sie können aber keine Betriebssystemdateien auf einem RAID-5-Volume speichern.

3. **Richtige Antwort: B**

A. **Falsch:** Wenn diese Richtlinie aktiviert ist, dürfen Remotebenutzer während ihrer Sitzung auf Wechselmediengeräte zugreifen. Sie dient nicht dazu, jeglichen Zugriff auf alle Arten externer Speichergeräte zu verweigern.

B. **Richtig:** Wenn diese Richtlinie aktiviert ist, wird jeglicher Zugriff auf alle Arten externer Speichergeräte verweigert. Sie überschreibt alle Zugriffsrechte, die durch andere Richtlinien gewährt werden.

C. **Falsch:** Wenn diese Richtlinie aktiviert ist, verweigert sie den Lesezugriff auf USB-Wechseldatenträger, portable Mediaplayer und Handys. Sie dient nicht dazu, jeglichen Zugriff auf alle Arten externer Speichergeräte zu verweigern.

D. **Falsch:** Wenn diese Richtlinie aktiviert ist, verweigert sie den Schreibzugriff auf USB-Wechseldatenträger, portable Mediaplayer und Handys. Sie dient nicht dazu, jeglichen Zugriff auf alle Arten externer Speichergeräte zu verweigern.

4. **Richtige Antwort: B**

A. **Falsch:** Um ein möglichst großes RAID-0-Volume (Stripesetvolume) zu erstellen, müssen Sie den Parameter `size` weglassen. Es funktioniert nicht, wenn Sie den Wert 0 übergeben.

B. **Richtig:** Dieser Befehl erstellt ein möglichst großes RAID-0-Volume.

C. **Falsch:** Der Befehl `create volume raid` erstellt ein RAID-5-Volume. Außerdem müssen Sie den Parameter `size` weglassen, um ein möglichst großes Volume zu erstellen.

D. **Falsch:** Dieser Befehl erstellt ein möglichst großes RAID-5-Volume.

5. **Richtige Antwort: D**

A. **Falsch:** Hätten Sie auf *Aberdeen* den Befehl `mountvol /n` oder `diskpart automount` ausgeführt, um zu verhindern, dass neue Volumes zum System hinzugefügt werden, würde das Volume nicht bereitgestellt und bekäme keinen Laufwerkbuchstaben. Es wird aber explizit erwähnt, dass dies nicht der Fall ist.

B. **Falsch:** Wenn Sie einen Basisdatenträger in einen anderen Computer einbauen, erhält er den nächsten freien Laufwerkbuchstaben auf diesem Computer. Sie verschieben aber einen dynamischen Datenträger.

C. **Falsch:** Der Laufwerkbuchstabe *G:* ist weder der nächste freie Buchstabe auf *Aberdeen* noch der Laufwerkbuchstabe, der dem Datenträger auf *Canberra* zugewiesen war. Es gibt keinen Grund, warum dem Datenträger dieser Laufwerkbuchstabe zugewiesen werden sollte.

D. **Richtig:** Werden dynamische Datenträger in andere Computer eingebaut, behalten sie den Laufwerkbuchstaben, den sie auf dem vorherigen Computer hatten, in diesem Fall also *H:*.

Kapitel 4: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Erzwingen einer Treibersignierungsrichtlinie

1. Das Tool DXdiag diagnostiziert alle Probleme im Zusammenhang mit einer Grafikkarte. Es verrät Ihnen unter anderem, ob der Treiber die WHQL-Tests bestanden hat.
2. Das Tool Sigverif durchsucht den Computer und meldet alle unsignierten Treiber.
3. Das Tool Msinfo32 listet die Ressourcen auf und zeigt an, welcher Treiber welche Ressourcen benutzt. Insbesondere sollten Sie den Knoten *Konflikte/Gemeinsame Nutzung* im Zweig *Hardwareressourcen* untersuchen.
4. Der Treiberüberprüfungs-Manager testet den Gerätetreiber unter konfigurierbaren Stressbedingungen.

Übung mit Fallbeispiel 2: Verwalten von Datenträgern

1. Erstellen Sie ein RAID-1-Array (gespiegeltes Volume) für Ihr Betriebssystem. Dabei spiegeln Sie Datenträger 0 in einem 200 GByte großen Bereich von Datenträger 2.
2. Erstellen Sie ein RAID-5-Volume (Stripesetvolume mit Parity), das den gesamten Platz auf Datenträger 1 und 3 (jeweils 200 GByte) sowie die 200 GByte nicht zugewiesenen Platz verwendet, die auf Datenträger 2 noch frei sind. Ein RAID-5-Volume bietet Fehlertoleranz und beschleunigt den Datenzugriff. Ein RAID-0-Array bietet zwar mehr Kapazität für die Datenspeicherung und steigert die Leistung noch weiter, es ist aber nicht fehlertolerant.
3. Drei 200 GByte große Abschnitte auf den unterschiedlichen Datenträgern ergeben ein RAID-5-Array mit 400 GByte nutzbarer Speicherkapazität.

Kapitel 5: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: A**
   A. **Richtig:** Sie sollten Windows XP Mode installieren und die Anwendung anschließend unter Windows XP installieren. Unter Windows XP Mode wird eine vollständig virtualisierte Kopie von Windows XP auf einem Computer ausgeführt, auf dem Windows 7 Professional, Enterprise oder Ultimate installiert ist. Anwendungen, die unter Windows XP funktionieren und unter Windows 7 Kompatibilitätsprobleme aufweisen, die sich nicht mit dem ACT lösen lassen, funktionieren gewöhnlich im Windows XP Mode.
   B. **Falsch:** Sie sollten keinen benutzerdefinierten Kompatibilitätsfix erstellen, weil aus der Frage bereits hervorgeht, dass sich kein passender Kompatibilitätsmodus entwickeln ließ. Ein Kompatibilitätsmodus ist eine Gruppe solcher Kompatibilitätsfixes.
   C. **Falsch:** Shim ist eine alte Bezeichnung für einen benutzerdefinierten Kompatibilitätsfix. Aus der Frage geht hervor, dass sich kein passender Kompatibilitätsmodus entwickeln ließ, der ja aus mehreren solcher Kompatibilitätsfixes besteht.
   D. **Falsch:** Sie sollten das Installationsprogramm der Anwendung nicht so konfigurieren, dass es im Modus Windows XP (Service Pack 2) ausgeführt wird, weil

Sie bereits festgestellt haben, dass Sie die Anwendung mit den Tools aus dem ACT nicht zum Laufen bringen. Das ACT bietet mehr Kompatibilitätsmodusoptionen, als in Windows 7 vordefiniert sind. Wenn eine Anwendung mit den vordefinierten Kompatibilitätsmodi von Windows 7 funktioniert, dann funktioniert sie mit den ACT-Modi allemal.

2. **Richtige Antwort: D**
   A. **Falsch:** Auch wenn die Anwendung vielleicht im Kompatibilitätsmodus Windows 98/Windows Me funktioniert, wissen Sie ja vorerst nur, dass die Anwendung unter Windows 2000 funktioniert. Daher sollten Sie diesen Kompatibilitätsmodus zuerst verwenden und nur dann andere Kompatibilitätsmodi ausprobieren, wenn sich der Modus Windows 2000 nicht eignet.
   B. **Falsch:** Auch wenn die Anwendung vielleicht im Kompatibilitätsmodus Windows NT 4 (Service Pack 5) funktioniert, wissen Sie ja vorerst nur, dass die Anwendung unter Windows 2000 funktioniert. Daher sollten Sie diesen Kompatibilitätsmodus zuerst verwenden und nur dann andere Kompatibilitätsmodi ausprobieren, wenn sich der Modus Windows 2000 nicht eignet.
   C. **Falsch:** Sie sollten den Kompatibilitätsmodus Windows XP (Service Pack 2) nicht einstellen, weil Sie wissen, dass die Anwendung nicht unter Windows XP funktioniert.
   D. **Richtig:** Sie sollten den Kompatibilitätsmodus Windows 2000 für die Anwendung einstellen, weil Sie wissen, dass die Anwendung unter Windows 2000 funktioniert.
3. **Richtige Antwort: B**
   A. **Falsch:** Sie können die Problembehandlung für Programmkompatibilität nicht für *.cab*-Dateien verwenden. Sie müssen den Inhalt der *.cab*-Datei extrahieren und die ausführbare Datei heraussuchen, die das Installationsprogramm der Anwendung enthält.
   B. **Richtig:** Die Problembehandlung für Programmkompatibilität funktioniert nur mit ausführbaren Dateien.
   C. **Falsch:** Sie können die Problembehandlung für Programmkompatibilität nicht für *.msi*-Installationsdateien verwenden. Die Problembehandlung für Programmkompatibilität funktioniert nur mit ausführbaren Dateien mit der Dateinamenerweiterung *.exe*.
   D. **Falsch:** Sie können die Problembehandlung für Programmkompatibilität nicht für *.zip*-Dateien verwenden. Sie müssen den Inhalt der *.zip*-Datei extrahieren und die ausführbare Datei heraussuchen, die das Installationsprogramm der Anwendung enthält.
4. **Richtige Antwort: C**
   A. **Falsch:** Sie sollten für die Anwendung nicht den Kompatibilitätsmodus Windows XP (Service Pack 3) einstellen, weil das Problem darin besteht, dass die Anwendung keine Anhebung der Rechte anfordert. Das ist auch in diesem Kompatibilitätsmodus der Fall.

B. **Falsch:** Sie sollten nicht den 256-Farbenmodus für die Anwendung einstellen. Diese Kompatibilitätsoption ist für Anwendungen vorgesehen, deren Darstellung auf dem Bildschirm nicht korrekt ist.

C. **Richtig:** Sie sollten die Kompatibilitätsoption *Programm als Administrator ausführen* aktivieren, wenn die Anwendung Administratorrechte braucht, aber keine Erhöhung der Rechte anfordern kann. Dann kann die Anwendung mit Administratorrechten ausgeführt werden, nachdem der Benutzer in der Bestätigungsaufforderung der Benutzerkontensteuerung seine Zustimmung gegeben hat.

D. **Falsch:** Sie sollten die Kompatibilitätsoption *Desktopgestaltung deaktivieren* nicht aktivieren. Verwenden Sie diese Option nur, wenn Sie die Benutzeroberfläche Aero während der Ausführung der Anwendung deaktivieren müssen.

5. **Richtige Antwort: B**

A. **Falsch:** Sie verwenden das IEAK zur Konfiguration des Internet Explorers. Dieses Toolkit eignet sich nicht dazu, die korrekte Darstellung einer vorhandenen Website im Internet Explorer 8 zu überprüfen, dem Standardbrowser von Windows 7.

B. **Richtig:** Das ACT enthält das Internet Explorer Compatibility Test Tool. Mit diesem Tool lässt sich überprüfen, ob eine Website zum Internet Explorer 8 kompatibel ist, dem Standardbrowser von Windows 7.

C. **Falsch:** Das Windows AIK enthält Tools für die Bereitstellung des Betriebssystems Windows. Damit können Sie nicht überprüfen, ob eine vorhandene Website im Internet Explorer 8, dem Standardbrowser von Windows 7, korrekt dargestellt wird.

D. **Falsch:** Das MDT unterstützt Sie bei der Planung und Bereitstellung von Betriebssystemen auf Clientcomputern. Damit können Sie nicht überprüfen, ob eine vorhandene Website im Internet Explorer 8, dem Standardbrowser von Windows 7, korrekt dargestellt wird.

Lektion 2

1. **Richtige Antwort: D**

A. **Falsch:** AppLocker eignet sich nicht, um die Ausführung von Anwendungen auf Computern zu verhindern, auf denen Windows Vista oder Windows 7 Professional verwendet wird.

B. **Falsch:** AppLocker eignet sich nicht, um die Ausführung von Anwendungen auf Computern zu verhindern, auf denen Windows Vista oder Windows 7 Professional verwendet wird.

C. **Falsch:** AppLocker eignet sich nicht, um die Ausführung von Anwendungen auf Computern zu verhindern, auf denen Windows Vista oder Windows 7 Professional verwendet wird.

D. **Richtig:** Da Sie die Ausführung von Anwendungen unter Windows Vista oder Windows 7 Professional nicht mit AppLocker verhindern können, müssen Sie dafür die Richtlinien für Softwareeinschränkung verwenden.

2. **Richtige Antwort: A**
   A. **Richtig:** Herausgeberregeln ermöglichen die Sperrung von Anwendungen auf der Basis des Herausgebers der Anwendung.
   B. **Falsch:** Pfadregeln ermöglichen nicht die Sperrung von Anwendungen auf der Basis des Herausgebers der Anwendung, wie in der Fragestellung verlangt. Sie ermöglichen die Sperrung einer ausführbaren Datei auf der Basis ihres Speicherorts.
   C. **Falsch:** Hashregeln ermöglichen nicht die Sperrung von Anwendungen auf der Basis des Herausgebers der Anwendung, wie in der Fragestellung verlangt. Sie ermöglichen die Sperrung einer bestimmten ausführbaren Datei auf der Basis eines Hashwerts, der aus der Datei errechnet wird.
3. **Richtige Antworten: B und C**
   A. **Falsch:** Sie sollten keine AppLocker-Herausgeberregeln erstellen. Herausgeberregeln lassen sich nur verwenden, wenn die betreffenden Dateien von den Herausgebern digital signiert wurden.
   B. **Richtig:** Sie sollten eine AppLocker-Hashregel erstellen, weil eine Herausgeberregel wegen der fehlenden digitalen Signatur nicht in Frage kommt.
   C. **Richtig:** Sie sollten die AppLocker-Überwachung der ausführbaren Regeln konfigurieren. Auf diese Weise können Sie überprüfen, ob die Regeln wie geplant funktionieren, bevor sie in einer Produktivumgebung wirksam werden.
   D. **Falsch:** Sie sollten keine AppLocker-Überwachung der Windows Installer-Regeln konfigurieren, weil Sie in diesem Fall an der korrekten Funktion der ausführbaren Regeln interessiert sind.
4. **Richtige Antwort: C**
   A. **Falsch:** Sie sollten die Gruppenrichtlinien nicht so konfigurieren, dass der Dienst *Anwendungsverwaltung* automatisch gestartet wird. Der Dienst *Anwendungsverwaltung* wird bei der Installation, Entfernung oder Auflistung von Software verwendet, die über Gruppenrichtlinien bereitgestellt wird. Der Dienst *Anwendungsidentität* ist es, der automatisch gestartet werden sollte.
   B. **Falsch:** Da die Richtlinien für Softwareeinschränkung korrekt funktionieren, brauchen Sie die Einstellungen der Dienste für die Computer, auf denen Windows 7 Professional verwendet wird, nicht zu ändern.
   C. **Richtig:** Damit die AppLocker-Richtlinien korrekt funktionieren, muss der Dienst *Anwendungsidentität* verfügbar sein. Dieser Dienst wird unter Windows 7 standardmäßig deaktiviert. In den Gruppenrichtlinien können Sie die Einstellung so ändern, dass der Dienst automatisch gestartet wird. Das wiederum ermöglicht die Durchsetzung der AppLocker-Richtlinien.
   D. **Falsch:** Da die Richtlinien für Softwareeinschränkung korrekt funktionieren, brauchen Sie die Einstellungen der Dienste für die Computer, auf denen Windows 7 Professional verwendet wird, nicht zu ändern.

5. **Richtige Antwort: A**
   A. **Richtig:** Sie müssen eine neue Hashregel für die Anwendung erstellen. Hashregeln müssen nach der Installation eines Updates für eine Anwendung aktualisiert werden, weil sich die ausführbare Datei bei diesem Vorgang gewöhnlich so ändert, dass der alte Dateihashwert nicht mehr gilt.
   B. **Falsch:** Da die Anwendung nicht digital signiert ist, können Sie keine AppLocker-Herausgeberregel verwenden.
   C. **Falsch:** Da die anderen AppLocker-Richtlinien funktionieren, kann man daraus schließen, dass der Dienst *Anwendungsidentität* verfügbar ist und seine Einstellung nicht geändert werden muss.
   D. **Falsch:** Der Dienst *Anwendungsverwaltung* wird bei der Installation, Entfernung oder Auflistung von Software verwendet, die über Gruppenrichtlinien bereitgestellt wird. Der Dienst hat keinen direkten Einfluss auf AppLocker-Richtlinien.

Kapitel 5: Antworten zu den Übungen mit Fallbeispiel

Übung 1: Konfigurieren der Anwendungskompatibilität bei Fabrikam

1. Bearbeiten Sie die Eigenschaften der Anwendung Alpha. Konfigurieren Sie die Anwendung so, dass sie im Kompatibilitätsmodus Windows XP (Service Pack 3) ausgeführt wird.
2. Bearbeiten Sie die Eigenschaften der Anwendung Beta. Aktivieren Sie auf der Registerkarte *Kompatibilität* das Kontrollkästchen *Programm als Administrator ausführen*. Dadurch wird die Anwendung immer als Administrator ausgeführt. Sie brauchen die Anwendung also nicht mehr bei jedem Start mit der rechten Maustaste anzuklicken, um diese Funktion zu aktivieren.
3. Sie können die Kompatibilitätsoptionen für die Anwendung Gamma mit dem ACT konfigurieren.

Übung 2: Beschränken von Anwendungen bei Contoso

1. Konfigurieren Sie eine ausführbare AppLocker-Regel, bei der ein Dateihashwert der Datenerfassungsanwendung verwendet wird. Eine Herausgeberregel kommt nicht in Frage, weil die Anwendung nicht digital signiert ist.
2. Konfigurieren Sie diese Regel für die Gruppe *Jeder*. Blockieren Sie die Ausführung der Anwendung, aber sehen Sie eine Ausnahme für die Gruppe *Scientists* vor.
3. Die Entwickler müssten die Anwendung digital signieren, damit Sie eine Herausgeberregel für die Anwendung erstellen könnten.

Kapitel 6: Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: C**
   A. **Falsch:** Mit dem Befehl `ping` wird die Konnektivität getestet. Er zeigt nicht die IP-Konfiguration der Schnittstellen eines Computers an.
   B. **Falsch:** Der Befehl `tracert` dient dazu, die Konnektivität zu einem Gerät in einem Remotenetzwerk zu testen. Er gibt Informationen über die dazwischen liegenden Hops zurück. Er zeigt nicht die IP-Konfiguration der Schnittstellen eines Computers an.
   C. **Richtig:** Der Befehl `ipconfig` zeigt die IP-Konfiguration der Schnittstellen eines Computers an.
   D. **Falsch:** Das Tool Netstat gibt Protokollstatistiken aus. Es zeigt nicht die IP-Konfiguration der Schnittstellen eines Computers an.
2. **Richtige Antworten: B, C und D**
   A. **Falsch:** Damit öffnen Sie das Dialogfeld *LAN-Einstellungen*. Sie können hier die automatische Konfiguration aktivieren, ein Skript für die automatische Konfiguration auswählen oder einen Proxyserver einstellen. Dieses Dialogfeld zeigt nicht die Verbindungseigenschaften an.
   B. **Richtig:** Damit öffnen Sie das Dialogfeld *Eigenschaften von LAN-Verbindung*.
   C. **Richtig:** Das ist eine andere Methode, um das Dialogfeld *Eigenschaften von LAN-Verbindung* zu öffnen.
   D. **Richtig:** Wenn Sie doppelt auf die LAN-Verbindung klicken, öffnet sich das Dialogfeld *Status von LAN-Verbindung*. Wenn Sie darin auf *Eigenschaften* klicken, öffnet sich das Dialogfeld *Eigenschaften von LAN-Verbindung*.
3. **Richtige Antwort: D**
   A. **Falsch:** DNS löst Computernamen in IP-Adressen auf. Sie geben beim Ping-Test aber die IPv4-Adressen der Computer an, nicht ihre Computernamen. Daher wird kein DNS-Dienst gebraucht, um die Befehle auszuführen.
   B. **Falsch:** Alle Computer im selben Subnetz müssen dieselbe Subnetzmaske haben.
   C. **Falsch:** Das Subnetz ist isoliert und es wird kein Gateway gebraucht, um Verkehr in andere Netzwerke zu senden. Sie brauchen kein Gateway zu definieren, um eine Verbindung zwischen zwei Computern innerhalb desselben Subnetzes herzustellen.
   D. **Richtig:** In der Standardeinstellung blockiert die Windows-Firewall den Befehl Ping. Sie müssen in beiden Firewalls ICMPv4-Verkehr erlauben. Geben Sie dazu auf beiden Computern in einer Eingabeaufforderung mit erhöhten Rechten den Befehl **netsh advfirewall firewall add rule name="ICMPv4"** ein.

4. **Richtige Antwort: B**
   A. **Falsch:** Damit legen Sie die Subnetzmaske /24 fest. Die Aufgabe beschreibt aber die Subnetzmaske /25 (255.255.255.128).
   B. **Richtig:** Damit konfigurieren Sie die statische IPv4-Adresse 10.0.10.162 im Subnetz 10.0.10.128/25.
   C. **Falsch:** Damit richten Sie eine dynamische Konfiguration ein.
   D. **Falsch:** Das Subnetz 10.0.10.128/25 hat den IPv4-Adressbereich 10.0.10.129 bis 10.0.10.254. Die IPv4-Adresse 10.0.10.16 liegt nicht in diesem Subnetz.
5. **Richtige Antworten: C und D**
   A. **Falsch:** Der Befehl `netsh interface ipv4 show route` zeigt Routentabelleneinträge an, aber nicht die IPv6-Routen.
   B. **Falsch:** Der Befehl `tracert -d` verfolgt den Weg eines IP-Pakets durch ein Internetzwerk. Es listet auf, welchen Pfad das Paket nimmt und welche Verzögerung bei jedem Abschnitt auftritt. Das Argument `-d` verhindert, dass das Tool IPv4-Adressen in Hostnamen auflöst. Der Befehl zeigt aber keine Routentabelle an.
   C. **Richtig:** Der Befehl `route print` zeigt die IPv4- und IPv6-Routentabellen an.
   D. **Richtig:** Der Befehl `netstat -r` liefert dieselben Informationen wie `route print`.
   E. **Falsch:** Der Befehl `netstat -a` zeigt alle aktiven Verbindungen sowie die vom Computer überwachten TCP- und UDP-Ports an. Er zeigt aber keine Routentabelle an.

Lektion 2

1. **Richtige Antwort: A**
   A. **Richtig:** Normalerweise verwenden Sie eine standortlokale Adresse. Hätte jedes Gerät im Subnetz eine globale Adresse, könnten Sie auch globale Adressen verwenden, aber diese Möglichkeit wird nicht als Antwort angeboten.
   B. **Falsch:** Wenn Sie verbindungslokale Adressen verwenden, müssen Sie ihre Schnittstellen-IDs angeben. Außerdem werden verbindungslokale Adressen nicht dynamisch in Windows-DDNS registriert. Daher ist es wesentlich einfacher, standortlokale Adressen zu verwenden; deshalb werden sie für diesen Zweck auch meist eingesetzt.
   C. **Falsch:** Es gibt nur zwei spezielle Adressen, nämlich :: und ::1. Beide eignen sich nicht, um IPv6-Konnektivität über ein privates Netzwerk zu implementieren.
   D. **Falsch:** Eine Anycastadresse wird nur auf einem Router konfiguriert. Sie kann keine IPv6-Konnektivität über ein privates Netzwerk implementieren. Außerdem ist sie keine Unicastadresse.
2. **Richtige Antwort: B**
   A. **Falsch:** Die Adresse fec0:0:0:0:fffe::1 ist eine standortlokale IPv6-Unicastadresse, die einen Knoten in einem Standort oder im Intranet identifiziert. Diese Art Adresse ist das Gegenstück zu einer privaten IPv4-Adresse (etwa 10.0.0.1). Sie ist nicht global routingfähig und nicht im IPv6-Internet erreichbar.

B. **Richtig:** Die Adresse 21cd:53::3ad:3f:af37:8d62 ist eine globale Unicastadresse. Dieser Adresstyp ist das IPv6-Gegenstück zur öffentlichen IPv4-Unicastadresse. Sie ist global routingfähig und im IPv6-Internet erreichbar.

C. **Falsch:** Die Adresse fe80:d1ff:d166:7888:2fd6 ist eine verbindungslokale IPv6-Unicastadresse, sie wird automatisch in einem lokalen Subnetz konfiguriert. Dies ist das Gegenstück zu einer APIPA-Adresse in IPv4 (z.B. 169.254.10.123). Sie ist nicht global routingfähig und nicht im IPv6-Internet erreichbar.

D. **Falsch:** Die Loopbackadresse ::1 identifiziert eine Loopbackschnittstelle, sie ist das Gegenstück zur IPv4-Loopbackadresse 127.0.0.1. Sie ist nicht global routingfähig und nicht im IPv6-Internet erreichbar.

3. **Richtige Antwort: D**

A. **Falsch:** ARP ist ein Protokoll, das mit Broadcasts arbeitet. In IPv4 werden damit IPv4-Adressen in MAC-Adressen aufgelöst. Es verwaltet nicht die Interaktion benachbarter Knoten und löst keine IPv6-Adressen in MAC-Adressen auf.

B. **Falsch:** DNS ist ein Dienst, kein Protokoll. Es löst Computernamen in IP-Adressen auf. Es verwaltet nicht die Interaktion benachbarter Knoten und löst keine IPv6-Adressen in MAC-Adressen auf.

C. **Falsch:** DHCPv6 weist statusbehaftete IPv6-Konfigurationen zu. Es verwaltet nicht die Interaktion benachbarter Knoten und löst keine IPv6-Adressen in MAC-Adressen auf.

D. **Richtig:** ND benutzt ICMPv6-Nachrichten, um die Interaktion benachbarter Knoten zu verwalten und IPv6-Adressen in MAC-Adressen aufzulösen.

4. **Richtige Antwort: A**

A. **Richtig:** Dies ist eine Teredo-Kompatibilitätsadresse. Teredo-Adressen beginnen mit 2001.

B. **Falsch:** Dies ist eine 6to4-Kompatibilitätsadresse. 6to4-Adressen beginnen mit 2002.

C. **Falsch:** Dies ist eine verbindungslokale ISATAP-Adresse. Sie erkennen sie an der Ziffernfolge 5efe, gefolgt von der hexadezimalen Darstellung einer IPv4-Adresse, in diesem Fall 10.0.2.143.

D. **Falsch:** Dies ist eine standortlokale IPv6-Adresse, keine IPv4-zu-IPv6-Kompatibilitätsadresse.

5. **Richtige Antwort: C**

A. **Falsch:** Ein PTR-Ressourceneintrag führt ein Reverse-Lookup durch und löst eine IPv4- oder IPv6-Adresse (abhängig von der angegebenen Reverse-Lookupzone) in einen Hostnamen auf.

B. **Falsch:** Ein A-Ressourceneintrag (address) löst einen Hostnamen in eine IPv4-Adresse auf.

C. **Richtig:** Ein AAAA-Ressourceneintrag löst einen Hostnamen in eine IPv6-Adresse auf.

D. **Falsch:** Ein Host-Ressourceneintrag ist eine andere Bezeichnung für einen A-Eintrag. Er löst einen Hostnamen in eine IPv4-Adresse auf.

Lektion 3

1. **Richtige Antwort: C**
   A. **Falsch:** Der Computer des Benutzers funktioniert im Büro einwandfrei. Es gibt keinen Grund, das Büronetzwerk neu zu konfigurieren.
   B. **Falsch:** In welcher Reihenfolge der Computer des Benutzers auf Netzwerke zugreift, ist hier egal. Das Problem tritt auf, wenn der Computer sich innerhalb der Reichweite von zwei Drahtlosnetzwerken befindet und zwischen den beiden umschaltet.
   C. **Richtig:** Die wahrscheinlichste Ursache für das gemeldete Verhalten ist, dass die Lobby des Hotels sich in der Reichweite von zwei Drahtlosnetzwerken befindet (vermutlich liegt sie genau dazwischen) und der Computer zwischen den beiden umschaltet. Sie können dieses Feature deaktivieren oder dem Benutzer erklären, wie das geht. Sie müssen den Benutzer warnen, dass er möglicherweise eine neue Verbindung zum Netzwerk herstellen muss, wenn er in einen anderen Teil des Hotels geht.
   D. **Falsch:** Das Notebook des Benutzers funktioniert im Büro und im Hotelzimmer einwandfrei. Mit dem Drahtlosadapter ist alles in Ordnung.
2. **Richtige Antwort: A**
   A. **Richtig:** Die MAC-Adresse identifiziert eine Schnittstelle eindeutig und ändert sich nicht. MAC-Adressfilterung stellt sicher, dass nur Computer, deren Drahtlosschnittstellen eine der eingetragenen MAC-Adressen haben, auf das Drahtlosnetzwerk zugreifen dürfen. Falls ein neuer Computer Zugriff auf das Netzwerk braucht oder Sie den Drahtlosadapter in einem Computer austauschen, müssen Sie allerdings die neue MAC-Adresse im WAP registrieren.
   B. **Falsch:** Die meisten Netzwerke werden mithilfe von DHCP konfiguriert, daher können sich die IPv4-Adressen ändern. Selbst in Netzwerken, wo IPv4-Adressen statisch konfiguriert sind, ist es unwahrscheinlich, dass der WAP IPv4-Adressfilterung unterstützt.
   C. **Falsch:** WEP ist eine Verschlüsselungsmethode, die sicherstellt, dass Nachrichten nicht ohne Weiteres gelesen werden können, selbst falls sie abgehört werden. Sie legt nicht fest, welche Computer auf ein Netzwerk zugreifen dürfen.
   D. **Falsch:** Wie WEP ist WPA eine Verschlüsselungsmethode. Sie legt nicht fest, welche Computer auf ein Netzwerk zugreifen dürfen.
3. **Richtige Antworten: C, E und F**
   A. **Falsch:** Das Windows-Netzwerkdiagnosetool ist kein Systemtool, es kann nicht über das Menü *Systemprogramme* geöffnet werden.
   B. **Falsch:** Das Windows-Netzwerkdiagnosetool führen Sie aus, wenn Sie ein Problem entdecken. Es ist kein Tool, das Sie regelmäßig ausführen lassen, und es befindet sich nicht in der Aufgabenplanungsbibliothek.
   C. **Richtig:** Sie können das Windows-Netzwerkdiagnosetool im Netzwerk- und Freigabecenter starten.

D. **Falsch:** Sie können im Eigenschaftendialogfeld eines Adapters nicht auf das Windows-Netzwerkdiagnosetool zugreifen. Dieses Dialogfeld wird für die Konfiguration verwendet, nicht für die Diagnose.

E. **Richtig:** Sie können das Windows-Netzwerkdiagnosetool ausführen, wenn der Zugriff auf eine Webseite fehlschlägt.

F. **Richtig:** Sie können das Windows-Netzwerkdiagnosetool für eine spezifische Verbindung ausführen, indem Sie das Dialogfeld *Netzwerkverbindungen* öffnen.

4. **Richtige Antwort: B**

A. **Falsch:** Die Windows-Firewall schützt Dons Computer, sie ist in der Standardeinstellung aktiviert. Seine Nachbarin greift aber auf seinen WAP zu, nicht auf seinen Computer.

B. **Richtig:** Das Setup des WAP war für Don so einfach, weil er alle Standardeinstellungen übernommen hat, ohne irgendwelche Sicherheitseinstellungen zu konfigurieren. Er muss die SSID ändern, Verschlüsselung konfigurieren und eine Passphrase eingeben. Außerdem sollte er das Zugriffskennwort ändern. Unter Umständen ist es auch sinnvoll, den Zugriff anhand der MAC-Adressen einzuschränken.

C. **Falsch:** Durch Umschalten des WAP-Kanals lassen sich möglicherweise Probleme beseitigen, die durch Störungen von Funktelefonen oder Mikrowellenherden (oder anderen Geräten) verursacht werden. Es hat keinen Einfluss darauf, wer auf das Netzwerk Zugriff hat.

D. **Falsch:** ICS ermöglicht es anderen Computern, ihre IPv4-Konfiguration vom ICS-Computer abzurufen. Sofern Don keine anderen Computer über Kabel mit seinem Drahtloscomputer verbunden hat, braucht er ICS nicht einzurichten. Weitere Drahtloscomputer erhalten ihre Konfigurationen direkt vom WAP. Dies hat keinen Einfluss darauf, dass seine Nachbarin auf sein Netzwerk Zugriff hat.

5. **Richtige Antwort: D**

A. **Falsch:** Damit wird *LaserF2* als Standarddrucker festgelegt, unabhängig davon, in welchem Stockwerk Sam sich befindet und mit welchem Netzwerk er verbunden ist. Das verursacht Probleme, weil Sam keine Verbindung zu *LaserF2* herstellen kann, während er sich im dritten Stock befindet.

B. **Falsch:** Damit wird *LaserF3* als Standarddrucker festgelegt, unabhängig davon, in welchem Stockwerk Sam sich befindet und mit welchem Netzwerk er verbunden ist. Das verursacht Probleme, weil Sam keine Verbindung zu *LaserF3* herstellen kann, während er sich im ersten Stock befindet.

C. **Falsch:** Damit wird *LaserF3* als Standarddrucker festgelegt, wenn Sam sich im ersten Stock befindet, und *LaserF2*, wenn sich Sam im dritten Stock aufhält. Das verursacht Probleme, weil *LaserF3* sich in einem Netzwerk befindet, das aus dem ersten Stock nicht erreichbar ist, und *LaserF2* in einem Netzwerk, das im dritten Stock nicht erreichbar ist.

D. **Richtig:** Damit wird *LaserF2* als Standarddrucker festgelegt, wenn Sam sich im ersten Stock befindet, und *LaserF3*, wenn sich Sam im dritten Stock aufhält. Das ist in dieser Aufgabe gefordert.

Kapitel 6: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Implementieren der IPv4-Konnektivität

1. Ihr Freund muss ICS auf dem Computer einrichten, an den sein Modem angeschlossen ist. Er muss sicherstellen, dass die anderen Computer im Netzwerk ihre IPv4-Konfiguration automatisch beziehen. Sobald er ICS auf dem ersten Computer konfiguriert hat, soll er die anderen beiden neu starten.
2. Er sollte den WAP über ein Ethernetkabel mit seinem DSL-Modem verbinden. Dann soll er die drei Desktopcomputer, die ein Kabelnetzwerk benutzen, an die Ethernetports des WAP anschließen und den WAP von einem dieser Computer aus über die Weboberfläche konfigurieren. Er kann den Drahtloscomputer im Netzwerk- und Freigabecenter mit seinem Netzwerk verbinden oder auf das Drahtlossymbol rechts unten auf seinem Bildschirm klicken.

Übung mit Fallbeispiel 2: Implementieren der IPv6-Konnektivität

1. Standortlokale IPv6-Adressen sind das direkte Gegenstück zu privaten IPv4-Adressen. Sie sind zwischen VLANs routingfähig. Es ist aber auch denkbar, alle Geräte in Ihrem Netzwerk mit zusammenfassbaren globalen Unicast-IPv6-Adressen zu konfigurieren. NAT und CIDR wurden eingeführt, um das Problem des knappen IPv4-Adressraums zu umgehen, und das ist in IPv6 kein Thema mehr. In diesem Fall ist es nicht möglich, ausschließlich verbindungslokale IPv6-Adressen zu verwenden, weil sie nicht routingfähig sind.
2. Das ist eine Teredo-Adresse, die mit einem Teredo-Tunnel verknüpft ist. Sie wird benutzt, um Kompatibilität zwischen IPv6 und IPv4 zu implementieren.

Übung mit Fallbeispiel 3: Verwenden von Windows 7-Notebooks in Drahtlosnetzwerken

1. Windows 7 führt das standortabhängige Drucken ein. Der Manager kann den Bürodrucker als Standarddrucker verwenden, während er bei Margie's Travel im Büro sitzt, und zu Hause seinen Tintenstrahldrucker als Standarddrucker. Die Umschaltung läuft nahtlos und automatisch, sofern beide Drucker als Standarddrucker eingerichtet sind.
2. Windows 7 hat einen neuen Assistenten zum Hinzufügen von Netzwerkdruckern. Er ist einfacher zu bedienen als der Assistent *Drucker hinzufügen*, und die Benutzer brauchen keine Administratorprivilegien, um Drucker zu installieren.
3. Der Angestellte hat Pech, weil sein Schreibtisch an einer Stelle steht, wo sich die beiden Drahtlosnetzwerke überschneiden. Sofern es nicht möglich ist, den Schreibtisch zu verlegen, können Sie die automatische Umschaltung deaktivieren. Damit wird das Problem beseitigt, aber Sie müssen den Angestellten warnen, dass er von Hand eine Netzwerkverbindung herstellen muss, wenn er sich in einen anderen Bereich des Gebäudes bewegt.

Kapitel 7: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: B**
   A. **Falsch:** Eingehende Regeln dienen dazu, Datenverkehr zu sperren, der aus dem Netzwerk stammt. Sie wollen aber eine bestimmte Art von Datenverkehr sperren, die vom Computer ausgeht und ins Netzwerk gesendet wird. Dafür brauchen Sie ausgehende Regeln.
   B. **Richtig:** Ausgehende Regeln ermöglichen es, Datenverkehr zu blockieren oder zuzulassen, der vom Computer in das Netzwerk gesendet wird. Sie sollen eine ausgehende Regel konfigurieren, die die Schüler daran hindert, mit FTP Dateien auf Internetsites hochzuladen, und eine weitere ausgehende Regel, die es den Schülern ermöglicht, mit SMTP E-Mails zu versenden.
   C. **Falsch:** Isolierungsregeln dienen dazu, die Hosts, mit denen ein Computer kommunizieren kann, auf die Hosts zu beschränken, die bestimmte Authentifizierungskriterien erfüllen. Sie eignen sich nicht zur Sperrung eines bestimmten Protokolls in ausgehenden Verbindungen.
   D. **Falsch:** Authentifizierungsausnahmeregeln werden zusammen mit Isolierungsregeln dafür verwendet, Verbindungen zuzulassen, ohne dass eine Authentifizierung erforderlich wäre. Authentifizierungsausnahmeregeln werden eher für eingehenden Datenverkehr als für ausgehenden verwendet.
2. **Richtige Antworten: B und C**
   A. **Falsch:** Die Windows-Firewall ermöglicht nicht die Erstellung von Firewallregeln für bestimmte Netzwerkorte auf der Basis von Portadressen. Mit der Windows-Firewall können Sie auch keine Regeln erstellen, die zwischen dem Heimnetzwerk und dem Arbeitsplatznetzwerk unterscheiden. Sie können nur Regeln erstellen, die zwischen privaten (Heim oder Arbeitsplatz) und öffentlichen Netzwerken unterscheiden.
   B. **Richtig:** Mit WFAS können Sie Firewallregeln auf der Basis der Portadresse und des Netzwerkortes erstellen.
   C. **Richtig:** WFAS-Regeln können Sie auch mit dem Befehlszeilenprogramm `Netsh` erstellen. WFAS-Regeln ermöglichen die Erstellung von Firewallregeln auf der Basis der Portadresse und des Netzwerkortes.
   D. **Falsch:** Netstat ist ein Tool, das Informationen über den Netzwerkdatenverkehr liefert. Mit Netstat können Sie keine Firewallregeln erstellen.
3. **Richtige Antwort: C**
   A. **Falsch:** Die beschriebene Regel blockiert keinen Datenverkehr, sondern lässt ihn zu.
   B. **Falsch:** Die beschriebene Regel gilt für eingehenden Datenverkehr, nicht für ausgehenden.
   C. **Richtig:** Diese Regel namens *BenutzerdefinierteRegel* gilt im Domänenprofil und lässt eingehenden TCP-Datenverkehr auf Port 80 zu. WFAS-Regeln können Sie auch mit Netsh im Kontext `advfirewall` erstellen.

D. **Falsch:** Die beschriebene Regel ist eine eingehende Regel, keine ausgehende Regel.

4. **Richtige Antwort: B**
   A. **Falsch:** Mit der Windows-Firewall können Sie zwar Regeln für Anwendungen erstellen, aber keine Regeln, die eine Authentifizierung von eingehenden Verbindungen verlangen.
   B. **Richtig:** WFAS ermöglicht die Erstellung von komplexen Regeln, die eingehenden Datenverkehr nur zulassen, wenn er authentifiziert wird.
   C. **Falsch:** Die Anmeldeinformationsverwaltung speichert Anmeldeinformationen. Sie eignet sich nicht zur Erstellung von Firewallregeln, die eine Authentifizierung verlangen.
   D. **Falsch:** Der Autorisierungs-Manager ermöglicht die Konfiguration von Rollen für die Delegierung von Administrationsrechten. Mit dem Autorisierungs-Manager können Sie keine Firewallregeln erstellen, die eine Authentifizierung verlangen.

5. **Richtige Antworten: A und D**
   A. **Richtig:** Sie sollten die Windows-Firewall im Bereich *Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)* so konfigurieren, dass Sie informiert werden, wenn ein Programm blockiert wird. Wenn dieses Netzwerkprofil wirksam ist, erhalten Sie eine Meldung, wenn ein neues Programm blockiert wird.
   B. **Falsch:** Sie sollten die Blockierungsmeldung im Bereich *Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)* nicht deaktivieren, weil Sie dann keine Meldung erhalten, wenn ein Programm blockiert wird.
   C. **Falsch:** Sie sollten die Blockierungsmeldung im Bereich *Standorteinstellungen für das öffentliche Netzwerk* nicht aktivieren, weil Sie dann eine Meldung erhalten, wenn ein neues Programm blockiert wird. Aus der Fragestellung geht aber hervor, dass dann keine Meldung angezeigt werden soll.
   D. **Richtig:** Sie sollten die Blockierungsmeldung im Bereich *Standorteinstellungen für das öffentliche Netzwerk* deaktivieren, weil dann keine Meldung mehr angezeigt wird, wenn ein Programm blockiert wird.

Lektion 2

1. **Richtige Antwort: C**
   A. **Falsch:** Sie sollten die Remoteunterstützung nicht aktivieren. Die Remoteunterstützung setzt voraus, dass jemand an dem Computer angemeldet ist, den Sie remote verwalten möchten.
   B. **Falsch:** Sie sollten die Option *Keine Verbindung mit diesem Computer zulassen* nicht aktivieren, weil Sie dann keine Remotedesktopverbindungen herstellen können.
   C. **Richtig:** Sie sollten die Option *Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird* aktivieren, damit Sie auf einem Computer, auf dem Windows XP mit SP2 ausgeführt wird, eine Remotedesktopverbindung mit einem Windows 7-Computer herstellen können.

D. **Falsch:** Sie sollen die Option *Verbindungen nur von Computern zulassen, die Remotedesktop mit Authentifizierung auf Netzwerkebene verwenden (höhere Sicherheit)* nicht aktivieren, weil Computer, auf denen Windows XP mit SP2 ausgeführt wird, sonst keine Verbindung mehr mit dem Windows 7-Computer herstellen können. Um eine Authentifizierung auf Netzwerkebene zu verwenden, muss auf Windows XP das Service Pack 3 installiert sein und eine spezielle Konfiguration erfolgen.

2. **Richtige Antwort: B**

   A. **Falsch:** Sie müssen Computer *Beta* und nicht Computer *Alpha* mit dem Befehl `WinRM quickconfig` konfigurieren.

   B. **Richtig:** Sie müssen auf Computer *Beta* den Befehl `WinRM quickconfig` verwenden, bevor Sie ihn auf Computer *Alpha* mit Windows PowerShell remote verwalten können. Dieser Befehl startet den WinRM-Dienst, konfiguriert einen Listener für die Ports, über die Windows-Remoteverwaltungsnachrichten gesendet und empfangen werden, und konfiguriert die Firewallausnahmen.

   C. **Falsch:** Es ist nicht erforderlich, auf dem Computer *Alpha* eine Firewallregel zu konfigurieren.

   D. **Falsch:** Es ist zwar nötig, auf Computer *Beta* eine Firewallregel zu erstellen, aber es ist ebenfalls nötig, einen Listener für die Windows-Remoteverwaltungsnachrichten zu konfigurieren und den WinRM-Dienst zu starten. Das kann alles mit dem Befehl `WinRM quickconfig` erledigt werden. Die Erstellung einer Firewallregel deckt nur einen Teil der erforderlichen Vorbereitungen ab.

3. **Richtige Antwort: B**

   A. **Falsch:** Der Befehl `nslookup` *`Aberdeen`* liefert zwar die IP-Adresse des Computers, aber nicht seine MAC-Adresse.

   B. **Richtig:** Der Befehl `winrs -r:`*`Aberdeen`* `ipconfig /all` führt auf *Aberdeen* den Befehl `ipconfig /all` aus, zeigt die Ergebnisse aber auf dem Computer an, an dem Sie angemeldet sind, in diesem Fall also auf *Canberra*. `Ipconfig /all` zeigt die MAC-Adresse (die »physische Adresse«) des Computers an.

   C. **Falsch:** Sie sollten nicht den Befehl `winrs -r:`*`Canberra`* `ipconfig /all` verwenden, weil er IP-Adressinformationen über den Computer *Canberra* liefert, nicht über den Computer *Aberdeen*.

   D. **Falsch:** Der Befehl `arp -a` zeigt Informationen über IP-Adressen und MAC-Adressen aus demselben Subnetz an, aber keine MAC-Adressinformationen über Computer aus Remotenetzen. Um mit diesem Befehl die MAC-Adresse eines anderen Computers zu ermitteln, müssen Sie die IP-Adressen dieses Computers kennen.

4. **Richtige Antwort: B**

   A. **Falsch:** Der Windows PowerShell-Befehl `icm Canberra {Get-Process}` zeigt Informationen über den Computer *Canberra* an, nicht über *Aberdeen*.

   B. **Richtig:** Der Windows PowerShell-Befehl `icm Aberdeen {Get-Process}` öffnet eine Windows PowerShell-Remotesitzung mit Computer *Aberdeen* und führt das Cmdlet `Get-Process` aus, das Prozessinformationen einschließlich Prozessor- und Speicherverwendung liefert.

C. **Falsch:** Mit WinRS können Sie kein Windows PowerShell-Cmdlet ausführen. Sie müssen Windows PowerShell mit der Syntax `icm Remotehost {PowerShell Cmdlet}` verwenden, um mit Windows PowerShell remote zu arbeiten.

D. **Falsch:** Mit WinRS können Sie kein Windows PowerShell-Cmdlet ausführen. Sie müssen Windows PowerShell mit der Syntax `icm Remotehost {PowerShell Cmdlet}` verwenden, um mit Windows PowerShell remote zu arbeiten. In diesem Beispiel richtet sich WinRS außerdem an den Computer *Canberra*, nicht an den Computer *Aberdeen*.

5. **Richtige Antwort: D**

A. **Falsch:** Der WinRM-Dienst wird für die Remoteverwendung von Windows PowerShell und Windows-Remoteshell gebraucht. Für die Remoteunterstützung ist der WinRM-Dienst nicht erforderlich.

B. **Falsch:** Ein Client muss nicht für Remotedesktopsitzungen konfiguriert werden, um mit Remoteunterstützung arbeiten zu können. Diese Einstellung erklärt also nicht, warum keine Verbindung zustande kommt. Windows 7-Clients unterstützen zudem eine Authentifizierung auf Netzwerkebene.

C. **Falsch:** Der Helfer braucht sich nicht auf dem Zielcomputer anzumelden, um eine Remoteunterstützungssitzung durchzuführen. Es spielt also keine Rolle, in welchen Gruppen das Benutzerkonto des Helfers Mitglied ist. Eine Remoteunterstützungssitzung ermöglicht dem Helfer, den Desktop des aktuell angemeldeten Benutzers zu sehen. Alles, was in dieser Sitzung getan wird, wird also mit den Berechtigungen des aktuell angemeldeten Benutzers getan.

D. **Richtig:** Wenn das Remoteunterstützungsprogramm geschlossen wird, sind keine Remoteunterstützungsverbindungen mehr möglich.

Kapitel 7: Antworten zu den Übungen mit Fallbeispiel

Übung 1: Client-Firewalls an einer Universität

1. Sie konfigurieren eine Windows-Firewallregel, die eingehenden Webdatenverkehr aus dem lokalen Subnetz zulässt. Teilnehmer der Konferenz können dann eine Verbindung zur Website herstellen, aber Benutzer aus anderen Netzwerken können dies nicht.
2. Sie sollten eine ausgehende Regel auf Portbasis erstellen, die das Dateiaustauschprogramm der Studenten blockiert. Mit Portregeln können Sie bestimmte Ports sperren. Das kann insbesondere dann von Nutzen sein, wenn die Programme, die diese Ports verwenden, verschiedene Identitäten annehmen.
3. Sie können auf einem Referenzcomputer einen Satz von Firewallregeln erstellen und diese Regeln auf ein USB-Flashlaufwerk exportieren. Anschließend importieren Sie die Firewallregeln auf jedem der eigenständigen Computer aus dem Kurs des Aufbaustudiums.

Übung 2: Desktopunterstützung in der Antarktis

1. Da zur Installation der Anwendung erhöhte Rechte erforderlich sind, stellen Sie eine Remotedesktopverbindung mit dem Windows 7-Client her und melden sich auf dem Client an.

2. Sie fügen das Konto des Mitarbeiters auf dem Windows 7-Client in der Forschungsstation zur Gruppe *Remotedesktopbenutzer* hinzu. Falls der Mitarbeiter im Büro in Tasmanien Windows XP verwendet, sorgen Sie dafür, dass auf dem Windows 7-Client in der Antarktis für Remotedesktopverbindungen keine Authentifizierung auf Netzwerkebene erforderlich ist.
3. Bevor Sie Windows PowerShell-Skripts für Windows 7-Remoteclients verwenden können, müssen Sie auf jedem Client in einer Eingabeaufforderung mit erhöhten Rechten den Befehl `WinRM quickconfig` verwenden.

Kapitel 8: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antworten: B, C und D**
   A. **Falsch:** Sie brauchen nicht alle einzelnen Datenordner freizugeben. Sie können die Ordner zu einer Bibliothek hinzufügen und diese Bibliothek dann für eine Heimnetzgruppe freigeben.
   B. **Richtig:** Sie sollten eine neue Bibliothek namens *Wissenschaftliche_Daten* erstellen, die separaten Datenordner der einzelnen Instrumente zu dieser Bibliothek hinzufügen und die Bibliothek dann auf der Seite *Heimnetzgruppe* der Systemsteuerung freigeben.
   C. **Richtig:** Sie sollten eine neue Bibliothek namens *Wissenschaftliche_Daten* erstellen, die separaten Datenordner der einzelnen Instrumente zu dieser Bibliothek hinzufügen und die Bibliothek dann auf der Seite *Heimnetzgruppe* der Systemsteuerung freigeben.
   D. **Richtig:** Sie sollten eine neue Bibliothek namens *Wissenschaftliche_Daten* erstellen, die separaten Datenordner der einzelnen Instrumente zu dieser Bibliothek hinzufügen und die Bibliothek dann auf der Seite *Heimnetzgruppe* der Systemsteuerung freigeben.
2. **Richtige Antwort: C**
   A. **Falsch:** Die Berechtigung *Drucken* ermöglicht Benutzern die Verwaltung der eigenen Dokumente, aber nicht die Verwaltung der Dokumente von anderen Benutzern.
   B. **Falsch:** Benutzer, denen Sie die Berechtigung *Diesen Drucker verwalten* zuweisen, sind in der Lage, die Druckerberechtigungen zu ändern. Sie sind nicht in der Lage, die Dokumente von anderen Benutzern direkt zu verwalten. Allerdings können sie sich selbst die Berechtigung *Dokumente verwalten* zuweisen und diese Aufgabe dann indirekt durchführen.
   C. **Richtig:** Wenn Sie einer Person die Berechtigung *Dokumente verwalten* zuweisen, kann sie die Reihenfolge aller in der Druckerwarteschlange befindlichen Dokumente ändern und die Druckaufträge löschen.
   D. **Falsch:** Die Gruppe *Hauptbenutzer* gibt es noch aus Gründen der Abwärtskompatibilität zu älteren Windows-Versionen. Die Zuweisung eines Benutzers zur Gruppe *Hauptbenutzer* erteilt dem Benutzer keine Druckerberechtigungen.

3. **Richtige Antworten: A und B**
   A. **Richtig:** Sie können den Befehl `net share` verwenden, um Freigabenamen und die dazugehörigen Ordnerpfade anzuzeigen.
   B. **Richtig:** Mit der Konsole *Computerverwaltung* können Sie die Namen und Ordnerpfade von Freigaben anzeigen.
   C. **Falsch:** Der Knoten *Bibliotheken* des Windows-Explorers ermöglicht die Konfiguration von Bibliotheken. Mit ihm können Sie nicht überprüfen, welche Freigaben es auf einem Windows 7-Computer gibt, weil es auch freigegebene Ordner geben kann, die nicht zu Bibliotheken gehören.
   D. **Falsch:** Sie können das Netzwerk- und Freigabecenter zur Konfiguration von Freigabeoptionen verwenden, aber es eignet sich nicht zur Überprüfung, welche freigegebenen Ordner es auf einem Windows 7-Computer gibt.
4. **Richtige Antwort: B**
   A. **Falsch:** Die Berechtigung *Lesen* reicht nicht aus. Wenn Sie diese Berechtigung zuweisen, können die Benutzer keine Dateien ändern oder löschen.
   B. **Richtig:** Sie sollten die Berechtigung *Ändern* zuweisen, weil Benutzer dadurch die Möglichkeit erhalten, Dateien zum freigegebenen Buchhaltungsordner hinzuzufügen, zu ändern oder zu löschen.
   C. **Falsch:** Sie sollten nicht die Berechtigung *Vollzugriff* zuweisen, weil die Benutzer dann die Freigabeberechtigungen des Ordners ändern können.
   D. **Falsch:** Sie können Gruppen nicht die Berechtigung *Besitzer* zuweisen. Bei der einfachen Freigabe weist Windows diese Berechtigung automatisch dem Benutzer zu, der den Ordner freigibt.
5. **Richtige Antwort: D**
   A. **Falsch:** Die Aktivierung dieser Option stellt nicht sicher, dass die freigegebenen Ressourcen für andere Computer aus der Heimnetzgruppe sichtbar sind. Diese Option ermöglicht es Benutzern im Netzwerk, Dateien aus dem öffentlichen Ordner zu lesen und in den Ordner zu schreiben.
   B. **Falsch:** Die Aktivierung dieser Option stellt nicht sicher, dass die freigegebenen Ressourcen für andere Computer aus der Heimnetzgruppe sichtbar sind. Diese Option ermöglicht eine Einstellung der Verschlüsselungsstufe von Dateifreigabeverbindungen.
   C. **Falsch:** Das kennwortgeschützte Freigeben beschränkt den Zugriff auf freigegebene Ressourcen eines Computers. Nur Benutzer, die auf dem Computer über ein lokales Konto verfügen, können auf freigegebene Ressourcen zugreifen, wenn das kennwortgeschützte Freigeben aktiviert ist. Die Aktivierung dieser Option stellt nicht sicher, dass die freigegebenen Ressourcen für andere Computer aus der Heimnetzgruppe sichtbar sind.
   D. **Richtig:** Die Netzwerkerkennung ermöglicht es einem Computer, andere Computer aus dem Netzwerk zu finden. Sie ermöglicht anderen Computern im Netzwerk zudem, die freigegebenen Ressourcen des Computers zu sehen.

Lektion 2

1. **Richtige Antwort: B**
   A. **Falsch:** Sie brauchen ein EFS-Zertifikat von Jeff, um eine Datei so zu verschlüsseln, dass er darauf zugreifen kann. Durch die Änderung des Kennworts wird kein EFS-Zertifikat erstellt.
   B. **Richtig:** Wenn Jeff eine Datei auf dem Computer verschlüsselt, wird ein EFS-Zertifikat für ihn erstellt. Sie können dieses EFS-Zertifikat verwenden, um die Datei für sein Konto zu verschlüsseln.
   C. **Falsch:** Jeff braucht keinen Schreibzugriff für eine Datei, damit Sie diese Datei für sein Konto verschlüsseln können. Sie brauchen ein Verschlüsselungszertifikat von Jeff, wie es erstellt wird, wenn Jeff auf dem Computer eine Datei verschlüsselt.
   D. **Falsch:** Wenn Jeff die Dateien in Besitz nimmt, können Sie sie nicht für sein Konto verschlüsseln. Sie brauchen ein Verschlüsselungszertifikat von Jeff, wie es erstellt wird, wenn Jeff auf dem Computer eine Datei verschlüsselt.
2. **Richtige Antworten: A und B**
   A. **Richtig:** Wenn Sie die Berechtigung *Lesen, Ausführen (Verweigern)* zuweisen, weist Windows automatisch auch die Berechtigungen *Ordnerinhalt anzeigen (Verweigern)* und *Lesen (Verweigern)* zu.
   B. **Richtig:** Wenn Sie die Berechtigung *Lesen, Ausführen (Verweigern)* zuweisen, weist Windows automatisch auch die Berechtigungen *Ordnerinhalt anzeigen (Verweigern)* und *Lesen (Verweigern)* zu.
   C. **Falsch:** Windows weist nicht die Berechtigung *Ändern (Verweigern)* zu, wenn Sie die Berechtigung *Lesen, Ausführen (Verweigern)* zuweisen.
   D. **Falsch:** Windows weist nicht die Berechtigung *Schreiben (Verweigern)* zu, wenn Sie die Berechtigung *Lesen, Ausführen (Verweigern)* zuweisen.
3. **Richtige Antwort: D**
   A. **Falsch:** Robocopy kann zum Kopieren von Dateien samt ihren NTFS-Berechtigungen verwendet werden, aber keine effektiven Berechtigungen ermitteln.
   B. **Falsch:** Icacls kann zwar zur Anzeige von Berechtigungen verwendet werden, aber nicht zur Ermittlung von effektiven Berechtigungen.
   C. **Falsch:** Cipher dient zur Verwaltung von Zertifikaten und eignet sich nicht zur Ermittlung von effektiven Berechtigungen.
   D. **Richtig:** Auf der Registerkarte *Effektive Berechtigungen* können Sie die effektiven Berechtigungen anzeigen, die sich beispielsweise durch die Mitgliedschaft in mehreren Gruppen ergeben.
4. **Richtige Antworten: A und D**
   A. **Richtig:** Verschlüsselte Dateien bleiben verschlüsselt, wenn sie in komprimierte Ordner kopiert oder verschoben werden.
   B. **Falsch:** Verschlüsselte Dateien bleiben verschlüsselt, wenn sie in komprimierte Ordner kopiert oder verschoben werden. Nur unverschlüsselte Dateien werden komprimiert, wenn sie in komprimierte Ordner kopiert oder verschoben werden.

C. **Falsch:** Dateien behalten ihre ursprünglichen NTFS-Berechtigungen nur, wenn sie zwischen Ordnern desselben Volumes verschoben werden. Wenn sie auf andere Volumes verschoben werden, erben sie die Berechtigungen des Zielordners. Mit Robocopy können Sie Dateien zwar mitsamt ihren NTFS-Berechtigungen verschieben, aber in der Frage wurde Robocopy nicht erwähnt.

D. **Richtig:** Dateien, die mit Windows-Explorer auf andere Volumes verschoben werden, erben die NTFS-Berechtigungen des Zielordners.

5. **Richtige Antwort: B**

A. **Falsch:** EFS eignet sich zur Beschränkung des Dateizugriffs auf bestimmte Benutzerkonten, gibt aber keine Auskunft darüber, welche Benutzer versucht haben, bestimmte Dateien zu verwenden.

B. **Richtig:** Durch eine entsprechende Überwachung können Sie ermitteln, welche Benutzerkonten für Datei- und Ordnerzugriffe verwendet wurden. Sie können die erfolgreichen und fehlgeschlagenen Versuche, die speziellen Berechtigungen zu verwenden, überwachen.

C. **Falsch:** Mit den NTFS-Berechtigungen können Sie nicht aufzeichnen, welche Benutzerkonten für Dokumentzugriffsversuche verwendet wurden, sondern nur festlegen, welche Benutzerkonten Zugriff auf Dokumente erhalten.

D. **Falsch:** BranchCache dient zur Beschleunigung des Dateizugriffs über WANs (Wide Area Networks) und eignet sich nicht dafür zu protokollieren, welche Benutzerkonten für Zugriffe auf Dokumente aus einem sensiblen Ordner verwendet werden.

Lektion 3

1. **Richtige Antworten: A und B**

A. **Richtig:** Der Modus »Gehosteter Cache« erfordert die Bereitstellung von mindestens einem Server in jeder Zweigstelle, auf dem Windows Server 2008 R2 ausgeführt wird und das Feature *BranchCache* aktiviert ist.

B. **Richtig:** Die Editionen Windows 7 Enterprise und Ultimate unterstützen BranchCache. Wenn Sie BranchCache verwenden möchten, müssen Sie die Clients auf eines dieser Betriebssysteme aktualisieren.

C. **Falsch:** Windows 7 Professional unterstützt BranchCache nicht.

D. **Falsch:** Ein Windows Server 2008-RODC ist zur Unterstützung von BranchCache nicht erforderlich.

2. **Richtige Antworten: B und D**

A. **Falsch:** Mit `net share` können Sie auf einem Windows 7-Client freigegebene Ordner verwalten, aber BranchCache weder aktivieren noch konfigurieren. Sie können ihn verwenden, um BranchCache für einen freigegebenen Ordner zu aktivieren, aber bevor Sie das tun können, muss BranchCache aktiviert und konfiguriert sein.

B. **Richtig:** Zur Konfiguration von BranchCache auf einem Windows 7-Client können Sie den Editor für lokale Gruppenrichtlinien und Netsh im BranchCache-Kontext verwenden.

C. **Falsch:** Ipconfig zeigt Informationen über die IP-Adressenkonfiguration an. Mit Ipconfig können Sie nicht BranchCache konfigurieren.

D. **Richtig:** Zur Konfiguration von BranchCache auf einem Windows 7-Client können Sie den Editor für lokale Gruppenrichtlinien und Netsh im BranchCache-Kontext verwenden.

3. **Richtige Antwort: C**

A. **Falsch:** Wenn Sie den Befehl `netsh branchcache set service disabled` verwenden, werden die über das WAN verfügbaren Inhalte nicht lokal zwischengespeichert.

B. **Falsch:** Wenn Sie den Befehl `netsh branchcache set service mode=distributed` verwenden, könnten andere Windows 7 Ultimate-Computer auf die Inhalte zugreifen. Bei entsprechender Konfiguration der Umgebung würden allerdings die Datei- und Ordnerberechtigungen den Zugriff verhindern.

C. **Richtig:** Sie sollten den Befehl `netsh branchcache set service mode=local` verwenden, weil der Windows 7 Ultimate-Computer dann Anforderungen aus seinem lokalen Zwischenspeicher bedienen kann, ohne ihn für andere Computer im Netzwerk zugänglich zu machen.

D. **Falsch:** Sie sollten nicht den Befehl `netsh branchcache set service mode=hosted-client location=fs-alpha.contoso.internal` verwenden. Den Modus `hostedclient` können Sie nur verwenden, wenn in Ihrem LAN ein Server mit aktiviertem BranchCache verfügbar ist, auf dem Windows Server 2008 R2 ausgeführt wird.

4. **Richtige Antwort: D**

A. **Falsch:** Der Befehl `netsh branchcache set service mode=distributed` stellt den Modus »Verteilter Cache« ein, nicht den Modus »Gehosteter Cache«. In der Frage wird aber der Modus »Gehosteter Cache« genannt.

B. **Falsch:** Der Befehl `netsh branchcache set service mode=local` konfiguriert den Client so, dass er einen lokalen Zwischenspeicher verwendet. Gefordert ist aber, dass die Clients den Modus »Gehosteter Cache« verwenden.

C. **Falsch:** Der Befehl `netsh branchcache set service mode=hostedserver clientauthentication=domain` dient zur Konfiguration des Hostservers und kann nicht zur Einstellung des Modus »Gehosteter Cache« auf Clients verwendet werden.

D. **Richtig:** Um einen BranchCache-Client so einzustellen, dass er im Modus »Gehosteter Cache« einen bestimmten Server benutzt, verwenden Sie den Befehl `netsh branchcache set service mode=hostedclient location=<Servername>`. Wenn Sie den Modus »Gehosteter Cache« konfigurieren, müssen Sie den Namen des lokalen Servers angeben, der als BranchCache-Host dient.

5. **Richtige Antwort: A**

A. **Richtig:** Die Richtlinie *BranchCache für Netzwerkdateien konfigurieren* ermöglicht die Angabe eines Latenzwertes, bei dessen Überschreitung Remotedateien auf den Clientcomputern der Zweigstelle zwischengespeichert werden.

B. **Falsch:** Mit der Richtlinie *Prozentuale Speicherplatzbelegung durch Clientcomputercache festlegen* wird die Größe des Zwischenspeichers festgelegt. Sie eignet sich nicht zur Einstellung des Latenzwertes.

C. **Falsch:** Mit der Richtlinie *BranchCache-Modus "Verteilter Cache" festlegen* wird der Modus »Verteilter Cache« eingestellt. Mit dieser Richtlinie können Sie keine Latenzwerte einstellen.

D. **Falsch:** Mit der Richtlinie *BranchCache-Modus "Gehosteter Cache" festlegen* wird der Modus »Gehosteter Cache« eingestellt. Mit dieser Richtlinie können Sie keine Latenzwerte einstellen.

Kapitel 8: Antworten zu den Übungen mit Fallbeispiel

Übung 1: Berechtigungen und Verschlüsselung

1. Sie exportieren den privaten Schlüssel des Benutzers vom Computer Waverley und importieren ihn auf dem Computer Warrandyte.
2. Sie erstellen mit *Cipher.exe* ein Wiederherstellungsagentzertifikat. Konfigurieren Sie dieses Zertifikat im Editor für lokale Gruppenrichtlinien als Wiederherstellungsagent.
3. Sie können *RoboCopy.exe* oder *Icacls.exe* verwenden, um die Dateien von einem Volume auf ein anderes zu verschieben und dabei die vorhandenen Berechtigungen beizubehalten. Wenn Sie die Dateien einfach nur verschieben, gehen die Berechtigungen verloren.

Übung 2: Konfigurieren der Contoso-Zweigstellen

1. In der Zweigstelle Wangaratta sollten Sie den Modus »Verteilter Cache« verwenden, weil an diesem Standort kein Server verfügbar ist, auf dem Windows Server 2008 R2 ausgeführt wird, und Windows Server 2008 BranchCache nicht unterstützt.
2. In der Zweigstelle Traralgon sollten Sie den Modus »Gehosteter Cache« verwenden, weil die Dateien auf diese Weise in einem zentralen Zwischenspeicher verfügbar gemacht werden. Der Zwischenspeicher kann stets online bleiben, im Gegensatz zum verteilen Zwischenspeicher, bei dem alle Clients online bleiben müssten. Am Standort Traralgon ist ein Server verfügbar, auf dem Windows Server 2008 R2 ausgeführt wird und der den Modus »Gehosteter Cache« unterstützen kann.
3. Installieren Sie auf dem Server das Feature *BranchCache* und sorgen Sie dafür, dass der freigegebene Ordner BranchCache unterstützt. Verwenden Sie auf dem Server den Befehl `netsh branchcache set service mode=hostedserver clientauthentication=domain`.

Kapitel 9: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: B**

   A. **Falsch:** Sie sollten die Einstellung *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus: Erhöhte Rechte ohne Eingabeaufforderung* nicht vornehmen. Diese Richtlinie gilt für alle Administratorkonten mit Ausnahme des vordefinierten Kontos *Administrator*, das mit anderen Richtlinien verwaltet werden muss.

   B. **Richtig:** Sie sollten die Richtlinie *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto* aktivieren. Dadurch errei-

chen Sie, dass für das vordefinierte *Administrator*-Konto eine Eingabeaufforderung der Benutzerkontensteuerung angezeigt wird, wenn mit diesem Konto eine Arbeit durchgeführt wird, die eine Erhöhung der Rechte erfordert.

C. **Falsch:** Sie sollten die Richtlinie *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto* nicht deaktivieren, weil dann für das vordefinierte *Administrator*-Konto keine Eingabeaufforderung der Benutzerkontensteuerung mehr angezeigt wird.

D. **Falsch:** Sie sollten die Einstellung *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus: Eingabeaufforderung zur Zustimmung für Nicht-Windows-Binärdateien* nicht vornehmen. Diese Richtlinie gilt für alle Administratorkonten mit Ausnahme des vordefinierten Kontos *Administrator*, das mit anderen Richtlinien verwaltet werden muss.

2. **Richtige Antwort: B**

A. **Falsch:** Sie sollten die Einstellung *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer: Anforderungen für erhöhte Rechte automatisch ablehnen* nicht vornehmen, weil Standardbenutzer dann keine Eingabeaufforderung der Benutzerkontensteuerung mehr erhalten, wenn sie eine Arbeit durchführen, für die eine Erhöhung der Rechte erforderlich ist. Die Erhöhung der Rechte wird dann automatisch abgelehnt.

B. **Richtig:** Sie sollten die Einstellung *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer: Eingabeaufforderung zu Anmeldeinformationen* vornehmen. Dann erhalten Standardbenutzer eine Aufforderung zur Eingabe von Anmeldeinformationen, wenn eine Erhöhung der Rechte erforderlich ist.

C. **Falsch:** Die Einstellung *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus: Eingabeaufforderung zu Anmeldeinformationen* sollten Sie nicht vornehmen, weil sie für Administratorkonten gilt, nicht für Standardbenutzerkonten.

D. **Falsch:** Sie sollten die Einstellung *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus: Eingabeaufforderung zur Zustimmung* nicht vornehmen, weil diese Richtline für Administratorkonten gilt, nicht für Standardbenutzerkonten. Außerdem wäre die Einstellung *Eingabeaufforderung zu Anmeldeinformationen* besser geeignet als die Einstellung *Eingabeaufforderung zur Zustimmung*.

3. **Richtige Antworten: A und D**

A. **Richtig:** Sie können für den Import und Export von Sicherheitsrichtlinien die Konsole *Editor für lokale Gruppenrichtlinien* verwenden. Damit können Sie die Richtlinien auf dem Referenzcomputer exportieren und dann auf jedem der 30 Computer des Computerkurses importieren.

B. **Falsch:** Die Konsole *Computerverwaltung* eignet sich nicht für den Import und Export von Gruppenrichtlinien.

C. **Falsch:** Das Dialogfeld *Einstellungen für Benutzerkontensteuerung* eignet sich nicht für den Import und Export von Gruppenrichtlinien.

D. **Richtig:** Sie können für den Import und Export von Sicherheitsrichtlinien die Konsole *Lokale Sicherheitsrichtlinie* verwenden. Damit können Sie die Richtlinien auf dem Referenzcomputer exportieren und dann auf jedem der 30 Computer des Computerkurses importieren.

4. **Richtige Antwort: D**

   A. **Falsch:** Die Richtlinie *Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind* hat nichts mit dem Schreiben von Daten an geschützten Orten zu tun. Sie ist für eine spezielle Gruppe von Anwendungen vorgesehen, die in ungewöhnlicher Weise mit dem Betriebssystem interagieren, und beschränkt die Ausführung der Anwendungen auf der Basis ihres Speicherorts.

   B. **Falsch:** Die Richtlinie *Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind* hat nichts mit dem Schreiben von Daten an geschützten Orten zu tun. Sie beschränkt die Anhebung der Rechte auf Anwendungen, die digital signiert wurden.

   C. **Falsch:** Die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer* hat nichts mit dem Schreiben von Daten an geschützten Orten zu tun. Sie dient zur Konfiguration der Benutzerkontensteuerung für Standardbenutzer.

   D. **Richtig:** Die Richtlinie *Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren* legt fest, ob Daten, die an geschützten Orten geschrieben werden sollen, umgeleitet werden. Eine Deaktivierung dieser Richtlinie bewirkt, dass ein Schreibversuch an einem geschützten Ort fehlschlägt.

5. **Richtige Antwort: C**

   A. **Falsch:** Sie sollten die Richtlinie *Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto* nicht konfigurieren. Sie steuert das Verhalten der Benutzerkontensteuerung, wenn das vordefinierte *Administrator*-Konto verwendet wird. Um Ihr Ziel zu erreichen, müssen Sie den Wechsel auf den sicheren Desktop deaktivieren.

   B. **Falsch:** Die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* ist bereits richtig konfiguriert. Um Ihr Ziel zu erreichen, müssen Sie den Wechsel auf den sicheren Desktop deaktivieren.

   C. **Richtig:** Sie müssen die Richtlinie *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln* deaktivieren. Wenn diese Richtlinie aktiviert ist, erscheint die Eingabeaufforderung der Benutzerkontensteuerung immer auf dem sicheren Desktop. Wird sie deaktiviert, hängt es von der Einstellung der Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* ab, ob die Eingabeaufforderung der Benutzerkontensteuerung auf dem sicheren Desktop erscheint.

   D. **Falsch:** Sie sollten die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer* nicht konfigurieren. Diese Richtlinie gilt für Standardbenutzer und hat nichts mit der Deaktivierung

des sicheren Desktops für Administratoren zu tun. Um Ihr Ziel zu erreichen, müssen Sie den Wechsel auf den sicheren Desktop deaktivieren.

Lektion 2

1. **Richtige Antwort: B**
   A. **Falsch:** Mit dem Befehl Runas können Sie keine gespeicherten Anmeldeinformationen entfernen. Dafür müssen Sie die Anmeldeinformationsverwaltung verwenden.
   B. **Richtig:** Mit der Anmeldeinformationsverwaltung können Sie Anmeldeinformationen entfernen, die vom Befehl Runas gespeichert wurden.
   C. **Falsch:** Mit der *Zertifikate*-Konsole können Sie keine gespeicherten Anmeldeinformationen entfernen. Die *Zertifikate*-Konsole dient zur Verwaltung von Zertifikaten.
   D. **Falsch:** Mit den Einstellungen für die Benutzerkontensteuerung können Sie keine gespeicherten Anmeldeinformationen entfernen. Im Dialogfeld *Einstellungen für Benutzerkontensteuerung* legen Sie fest, in welchen Situationen Eingabeaufforderungen der Benutzerkontensteuerung erfolgen sollen.
2. **Richtige Antworten: C und D**
   A. **Falsch:** Sie sollten die Richtlinieneinstellung *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards: Keine Aktion* nicht vornehmen, weil die Benutzer dann angemeldet bleiben, wenn sie ihre Smartcards entfernen.
   B. **Falsch:** Sie sollten die Richtlinieneinstellung *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards: Arbeitsstation sperren* nicht vornehmen, weil ein Benutzer dann nicht abgemeldet wird, wenn er seine Smartcards entfernt. Stattdessen wird seine Arbeitsstation gesperrt.
   C. **Richtig:** Sie sollten die Richtlinieneinstellung *Interaktive Anmeldung: Verhalten bei Entfernen von Smartcards: Abmeldung erzwingen* vornehmen, wenn Sie wollen, dass Benutzer, die ihre Smartcard entfernen, automatisch abgemeldet werden.
   D. **Richtig:** Sie sollten die Richtlinieneinstellung *Interaktive Anmeldung: Smartcard erforderlich: Aktiviert* vornehmen, weil sich Benutzer dann nur noch mit Smartcard anmelden können.
3. **Richtige Antwort: B**
   A. **Falsch:** Aus der Frage geht nicht hervor, ob das Konto gesperrt wurde. Es wird nur gesagt, dass der Benutzer sein Kennwort vergessen hat. Eine Aufhebung der Kontosperre reicht nur aus, wenn der Benutzer sein Kennwort noch kennt. Dadurch wird das Kennwort nicht zurückgesetzt.
   B. **Richtig:** Sie müssen das Kennwort zurücksetzen. Dabei verliert der Benutzer den Zugang zu seinen verschlüsselten Dateien, falls er seinen EFS-Schlüssel nicht gesichert hat. Außerdem verliert der Benutzer den Zugang zu den Anmeldeinformationen, die im Windows-Tresor gespeichert wurden.
   C. **Falsch:** Sie können nur für ein Konto, dessen Kennwort Sie kennen, eine Kennwortrücksetzdiskette erstellen. Für das Konto eines Benutzers, der sein Kennwort vergessen hat, können Sie nicht nachträglich eine Kennwortrücksetzdiskette erstellen.

D. **Falsch:** Wenn Sie eine Kennwortrücksetzdiskette für Ihr eigenes Konto erstellen, ist das Problem des Benutzers nicht behoben.

4. **Richtige Antwort: D**
   A. **Falsch:** Die Richtlinie *Kennwortchronik erzwingen* bewirkt, dass ein Benutzer bei der Kennwortänderung kein Kennwort wählen kann, das er kürzlich verwendet hat. Sie sorgt nicht dafür, dass ein Benutzer nach einer bestimmten Zeitspanne sein Kennwort ändern muss.
   B. **Falsch:** Die Richtlinie *Minimale Kennwortlänge* lässt keine Kennwörter zu, die eine Mindestlänge unterschreiten. Sie sorgt nicht dafür, dass ein Benutzer nach einer bestimmten Zeitspanne sein Kennwort ändern muss.
   C. **Falsch:** Die Richtlinie *Minimales Kennwortalter* bewirkt, dass ein Benutzer sein Kennwort in dem angegebenen Zeitraum nicht erneut ändern kann. Sie sorgt nicht dafür, dass ein Benutzer nach einer bestimmten Zeitspanne sein Kennwort ändert.
   D. **Richtig:** Die Richtlinie *Maximales Kennwortalter* sorgt dafür, dass ein Benutzer sein Kennwort nach Ablauf des angegebenen Zeitraums ändern muss. In diesem Fall würden Sie 21 Tage einstellen.

5. **Richtige Antworten: B, C und D**
   A. **Falsch:** Die Anmeldeinformationsverwaltung kann Anmeldeinformationen für Websites, Benutzernamen und Kennwörter sowie bestimmte Arten von digitalen Zertifikaten sichern, aber keine selbstsignierten EFS-Zertifikate, wie sie von Windows 7 erstellt werden, wenn Sie zum ersten Mal eine Datei verschlüsseln.
   B. **Richtig:** Mit dem Tool *Dateiverschlüsselungszertifikate verwalten* können Sie EFS-Zertifikate in einer kennwortgeschützten PFX-Datei sichern.
   C. **Richtig:** Mit der Konsole *Zertifikate* können Sie ein EFS-Zertifikat in eine kennwortgeschützte PFX-Datei exportieren.
   D. **Richtig:** Mit dem Befehlszeilentool *Cipher.exe* können Sie EFS-Zertifikate in einer kennwortgeschützten PFX-Datei sichern.

Kapitel 9: Antworten zu den Übungen mit Fallbeispiel

Übung 1: Benutzerkontensteuerung bei Coho Vineyard

1. Sie müssen die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus* auf *Eingabeaufforderung zu Anmeldeinformationen* stellen. Außerdem müssen Sie die Richtlinie *Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln* deaktivieren. Dadurch erreichen Sie, dass Administratoren zwar zur Eingabe ihrer Anmeldeinformationen aufgefordert werden, aber nicht sofort auf diese Aufforderung reagieren müssen.
2. Sie müssen die Richtlinie *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer* so einstellen, dass Benutzer zur Eingabe von Anmeldeinformationen aufgefordert werden, wenn sie eine Arbeit durchführen wollen, die erhöhte Rechte erfordert. Außerdem müssen Sie die Richtlinie *Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desk-*

top anfordern aktivieren. Dann können Helfer auf die Eingabeaufforderung der Benutzerkontensteuerung reagieren, wenn sie über UIAccess-Anwendungen angemeldet sind.

3. Sie müssen die Richtlinie *Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind* aktivieren. Diese Richtlinie können Sie verwenden, weil alle bei Coho Vineyard verwendeten Anwendungen, die erhöhte Rechte anfordern könnten, digital signiert sind.

Übung 2: Beheben von Kennwortproblemen bei Wingtip Toys

1. Sorgen Sie dafür, dass die Benutzer ihre EFS-Schlüssel sichern. Dazu können sie *Cipher.exe*, das Tool *Dateiverschlüsselungszertifikate verwalten* oder *Certmgr.msc* verwenden. Außerdem sollten die Benutzer ihre gespeicherten Website-Kennwörter mit der Anmeldeinformationsverwaltung sichern.
2. Bringen Sie die Benutzer dazu, Kennwortrücksetzdatenträger zu erstellen.
3. Konfigurieren Sie die Richtlinien *Maximales Kennwortalter* und *Kennwortchronik erzwingen*.

Kapitel 10: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: D**
   A. **Falsch:** Teredo ist geeignet, wenn ein Client über eine private IPv4-Adresse verfügt und keine Firewall den Datenverkehr auf UDP-Port 3544 blockiert. Da dieser Port blockiert wird, verwendet der Client IP-HTTPS.
   B. **Falsch:** Zur Verwendung von IP6-zu-IP4 muss der Client über eine öffentliche IPv4-Adresse verfügen. Aus der Frage geht hervor, dass dem Client eine private IPv4-Adresse zugewiesen wurde.
   C. **Falsch:** Um eine global routbare IPv6-Adresse verwenden zu können, muss dem Client eine global routbare IPv6-Adresse zugewiesen werden.
   D. **Richtig:** IP-HTTPS wird verwendet, wenn dem Client in einem Netzwerk, das Internetzugang ermöglicht, das aber durch eine Firewall geschützt wird, die den größten Teil des Netzwerkdatenverkehrs blockiert, eine private IPv4-Adresse zugewiesen wird.
2. **Richtige Antworten: A und B**
   A. **Richtig:** Nur die Editionen Windows 7 Ultimate und Enterprise unterstützen DirectAccess.
   B. **Richtig:** Nur Windows 7-Client, die Mitglieder von Domänen sind, können DirectAccess verwenden.
   C. **Falsch:** AppLocker-Richtlinien legen fest, welche Anwendungen auf einem Windows 7-Client ausgeführt werden können. Sie haben nichts mit DirectAccess zu tun.
   D. **Falsch:** BranchCache-Richtlinien ermöglichen Clients, die sich in Zweigstellen befinden, WAN-Inhalte lokal zwischenzuspeichern. Sie haben nichts mit DirectAccess zu tun.

3. **Richtige Antwort: A**
   A. **Richtig:** Der DirectAccess-Server muss mit zwei Netzwerkkarten ausgerüstet sein und über zwei aufeinanderfolgende öffentliche IPv4-Adressen verfügen.
   B. **Falsch:** Der DirectAccess-Server muss über zwei Netzwerkkarten verfügen. Eine Netzwerkkarte ist für das interne Netzwerk vorgesehen und die andere muss über das Internet zugänglich sein.
   C. **Falsch:** Dem DirectAccess-Server müssen zwei aufeinanderfolgende öffentliche IPv4-Adressen zugewiesen werden.
   D. **Falsch:** Der DirectAccess-Server muss über zwei Netzwerkkarten verfügen. Eine Netzwerkkarte ist für das interne Netzwerk vorgesehen und die andere muss über das Internet zugänglich sein.
4. **Richtige Antwort: A**
   A. **Richtig:** DirectAccess konfiguriert spezielle Gruppenrichtlinienobjekte mit den Einstellungen für DirectAccess. Diese Gruppenrichtlinienobjekte werden auf bestimmte Sicherheitsgruppen angewendet, die Computerkonten enthalten. Damit ein Computer DirectAccess benutzen kann, muss er Mitglied einer dieser speziellen Sicherheitsgruppen sein.
   B. **Falsch:** Die Konfiguration von DirectAccess erfolgt durch die Anwendung von Gruppenrichtlinien auf die Konten von Computern, die Domänenmitglieder sind. Lokale Gruppenmitgliedschaften sind dafür nicht von Bedeutung.
   C. **Falsch:** Das Computerkonto muss Mitglied der Domänensicherheitsgruppe sein, nicht das Benutzerkonto.
   D. **Falsch:** Das Computerkonto muss Mitglied der Domänensicherheitsgruppe sein. Für DirectAccess ist es nicht wichtig, welcher lokalen Gruppe ein Benutzerkonto angehört.
5. **Richtige Antwort: D**
   A. **Falsch:** Der Befehl `ipconfig` zeigt die IP-Adressenkonfiguration an. Er zeigt keine Informationen über die DirectAccess-IP-HTTPS-Serverkonfiguration an.
   B. **Falsch:** Der Befehl `netsh interface 6to4 show relay` zeigt IP6-zu-IP4-Informationen. IP6-zu-IP4 kann verwendet werden, wenn einem Computer eine öffentliche Adresse zugewiesen wurde, also keine private Adresse, und er sich nicht hinter einem NAT-Gerät befindet.
   C. **Falsch:** Der Befehl `Netsh interface ipv6 show teredo` zeigt Teredo-Informationen. Teredo kann nicht verwendet werden, wenn eine Hotel-Firewall sämtlichen Datenverkehr blockiert, der nicht über die Ports 80 und 443 erfolgt.
   D. **Richtig:** Der Befehl `Netsh interface httpstunnel show interfaces` zeigt Informationen über die DirectAccess-IP-HTTPS-Konfiguration.

Lektion 2

1. **Richtige Antwort: D**
   A. **Falsch:** PPTP-VPNs unterstützen unter Windows 7 kein VPN-Reconnect.
   B. **Falsch:** L2TP/IPsec-VPNs unterstützen unter Windows 7 kein VPN-Reconnect.
   C. **Falsch:** SSTP-VPNs unterstützen unter Windows 7 kein VPN-Reconnect.

D. **Richtig:** Der VPN-Typ IKEv2 ist der einzige VPN-Typ, der unter Windows 7 VPN-Reconnect unterstützt.

2. **Richtige Antwort: A**
   A. **Richtig:** SSTP-VPN-Verbindungen verwenden dieselben Ports wie sichere Webbrowserverbindungen. Das ermöglicht Benutzern, die mit der Internetverbindung eines Hotels im Web browsen können, gewöhnlich eine Verbindung über VPN.
   B. **Falsch:** IKEv2 verwendet den UDP-Port 500, der wahrscheinlich ebenfalls blockiert wird, wenn eine Firewall alle anderen Datenverkehrsformen bis auf die gebräuchlichsten Protokolle blockiert, die von Webbrowsern verwendet werden.
   C. **Falsch:** PPTP verwendet Port 1723, der wahrscheinlich ebenfalls blockiert wird, wenn eine Firewall alle anderen Datenverkehrsformen bis auf die gebräuchlichsten Protokolle blockiert, die von Webbrowsern verwendet werden.
   D. **Falsch:** L2TP/IPsec verwendet UDP-Port 1701, der wahrscheinlich ebenfalls blockiert wird, wenn eine Firewall alle anderen Datenverkehrsformen bis auf die gebräuchlichsten Protokolle blockiert, die von Webbrowsern verwendet werden.

3. **Richtige Antworten: C und D**
   A. **Falsch:** SSTP wird nur von Routing- und RAS-Servern unter Windows Server 2008 und Windows Server 2008 R2 unterstützt.
   B. **Falsch:** IKEv2 wird nur von Routing- und RAS-Servern unter Windows Server 2008 R2 unterstützt.
   C. **Richtig:** PPTP wird von Routing- und RAS-Servern unter Windows Server 2003 R2 unterstützt.
   D. **Richtig:** L2TP/IPsec wird von Routing- und RAS-Servern unter Windows Server 2003 R2 unterstützt.

4. **Richtige Antworten: A, B und C**
   A. **Richtig:** Sie können das PEAP-Authentifizierungsprotokoll für ein IKEv2-VPN verwenden.
   B. **Richtig:** Sie können das EAP-MSCHAP v2-Authentifizierungsprotokoll für ein IKEv2-VPN verwenden.
   C. **Richtig:** Sie können in einem IKEv2-VPN eine Smartcard oder ein anderes Zertifikat zur Authentifizierung verwenden.
   D. **Falsch:** In einem IKEv2-VPN können Sie nicht das CHAP-Protokoll verwenden. IKEv2-VPNs lassen sich nur mit EAP oder Computerzertifikaten authentifizieren.

5. **Richtige Antwort: C**
   A. **Falsch:** DirectAccess ist unter Windows 7 Professional nicht verfügbar. Wäre DirectAccess verfügbar, würde diese Lösung funktionieren.
   B. **Falsch:** Sie sollten Remotedesktopverbindung nicht so konfigurieren, dass es ein Remotedesktopgateway *remote-desktop.contoso.internal* verwendet und dann eine Verbindung zu *rdgateway.contoso.com* herstellt, denn *rdgateway.contoso.com* ist das Remotedesktopgateway. In dieser Antwort sind Remotedesktop-Gatewayserver und Remotedesktopdiensteserver vertauscht.

C. **Richtig:** Konfigurieren Sie Remotedesktopverbindung so, dass es das Remotedesktopgateway *rdgateway.contoso.com* verwendet. Stellen Sie dann eine Verbindung zu *remote-desktop.contoso.internal* her.

D. **Falsch:** DirectAccess ist unter Windows 7 Professional nicht verfügbar. Wäre es verfügbar, müssten Sie eine Verbindung zu *remote-desktop.contoso.internal* herstellen, nicht zum Remotedesktop-Gatewayserver.

Kapitel 10: Antworten zu den Übungen mit Fallbeispiel

Übung 1: DirectAccess bei Wingtip Toys

1. Aktualisieren Sie den Server auf Windows Server 2008 R2. Die restliche Konfiguration des Servers unterstützt DirectAccess, weil der Server Mitglied einer Domäne ist, auf seiner Internetschnittstelle über zwei aufeinanderfolgende IP-Adressen verfügt und auch schon das passende Computerzertifikat vorweisen kann. Nach der Aktualisierung des Servers auf das neue Betriebssystem können Sie DirectAccess installieren.
2. Sie sollten in der Wingtip Toys-Domäne eine globale Sicherheitsgruppe erstellen.
3. Aktualisieren Sie die Clientcomputer auf Windows 7 Enterprise oder Ultimate. Fügen Sie die Computerkonten zu der Sicherheitsgruppe hinzu, die Sie für DirectAccess erstellt haben. Installieren Sie die Computerzertifikate.

Übung 2: Remote Access bei Tailspin Toys

1. Windows 7 Enterprise unterstützt zwar IKEv2-VPNs, aber ein Routing- und RAS-Server unter Windows Server 2003 R2 tut dies nicht. Zur Unterstützung von IKEv2-VPNs ist es erforderlich, den Routing- und RAS-Server auf Windows Server 2008 R2 zu aktualisieren.
2. Installieren Sie im Quarantänenetzwerk einen Antiviren-Updateserver und einen WSUS-Server, damit Clients sich selbst aktualisieren können, um wieder den Integritätsanforderungen zu genügen.
3. Sie sollten das EAP-MS-CHAPv2-Authentifizierungsprotokoll verwenden, weil es eine Authentifizierung auf Kennwortbasis ermöglicht.

Kapitel 11: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antworten: A, D und E**

   A. **Richtig:** Ein BitLocker-verschlüsseltes Volume muss mit einer eindeutigen Kennung versehen werden, damit ein DRA verwendet werden kann. Um diese Kennung zuzuweisen, müssen Sie die Richtlinie *Eindeutige IDs für Ihre Organisation angeben* konfigurieren.

   B. **Falsch:** Die Richtlinie *Standardordner für Wiederherstellungskennwort auswählen* lässt die Speicherung des Wiederherstellungskennworts an einem bestimmten Ort zu. Für einen DRA wird dagegen ein spezielles Zertifikat verwendet, das dazu verwendet werden kann, um alle BitLocker-verschlüsselten Volumes einer Organisation wiederherzustellen.

C. **Falsch:** Die Richtlinie *Wiederherstellungsoptionen für BitLocker-geschützte Laufwerke für Benutzer auswählen* legt fest, ob eine Wiederherstellung mit einem Kennwort oder mit einem USB-Flashlaufwerk und Schlüssel erfolgt. Für einen DRA wird dagegen ein spezielles Zertifikat verwendet, das dazu verwendet werden kann, um alle BitLocker-verschlüsselten Volumes einer Organisation wiederherzustellen.

D. **Richtig:** Damit BitLocker DRAs unterstützt, müssen Sie den DRA mit der Richtlinie *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel\BitLocker-Laufwerkverschlüsselung* konfigurieren.

E. **Richtig:** Sie müssen die Richtlinie *Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können* konfigurieren und angeben, dass ein DRA zur Wiederherstellung von geschützten Betriebssystemvolumes verwendet werden kann.

2. **Richtige Antworten: C und D**

A. **Falsch:** Die Richtlinie *Verwendung von BitLocker auf Wechseldatenträgern steuern* ermöglicht die Verwendung von BitLocker auf Wechseldatenträgern. Mit dieser Richtlinie können Sie nicht die Verwendung von Wechseldatenträgern auf Geräte einschränken, die mit BitLocker geschützt werden.

B. **Falsch:** Die Richtlinie *BitLocker-Wiederherstellungsinformationen in Active Directory-Domänendiensten speichern*, die für Windows Vista-Clients gilt und nicht für Windows 7, ermöglicht die Speicherung von BitLocker-Wiederherstellungsschlüsseln in AD DS. Mit dieser Richtlinie können Sie nicht die Verwendung von Wechseldatenträgern auf Geräte einschränken, die mit BitLocker geschützt werden.

C. **Richtig:** Sie müssen die Richtlinie *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind* konfigurieren. Die Richtlinie ermöglicht es, Schreibzugriffe auf Laufwerke zu sperren, die nicht mit BitLocker geschützt werden oder die in anderen Organisationen konfiguriert wurden.

D. **Richtig:** Die Richtlinie *Eindeutige IDs für Ihre Organisation angeben* ermöglicht die Festlegung von BitLocker-Kennungen für eine Organisation. Schreibzugriffe lassen sich mit diesen Kennungen und durch eine entsprechende Konfiguration der Richtlinie *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind* auf Wechselgeräte beschränken, die aus der Organisation stammen.

3. **Richtige Antwort: A**

A. **Richtig:** Durch eine entsprechende Konfiguration der Richtlinie *Zusätzliche Authentifizierung beim Start anfordern* ist es möglich, BitLocker auch auf Computern zu verwenden, die nicht über einen TPM-Chip verfügen.

B. **Falsch:** Die Richtlinie *Erweiterte PINs für Systemstart zulassen* ermöglicht die Verwendung einer erweiterten PIN beim Start des Computers. Eine Konfiguration dieser Richtlinie ermöglicht nicht die Verwendung von BitLocker auf Computern, die nicht über einen TPM-Chip verfügen.

C. **Falsch:** Mit der Richtlinie *TPM-Plattformvalidierungsprofil konfigurieren* wird festgelegt, wie der TPM-Chip den BitLocker-Verschlüsselungsschlüssel sichert.

Eine Konfiguration dieser Richtlinie ermöglicht nicht die Verwendung von BitLocker auf Computern, die nicht über einen TPM-Chip verfügen.

D. **Falsch:** Die Richtlinie *Minimale PIN-Länge für Systemstart konfigurieren* ermöglicht die Festlegung einer Mindestlänge für die Start-PIN. Eine Konfiguration dieser Richtlinie ermöglicht nicht die Verwendung von BitLocker auf Computern, die nicht über einen TPM-Chip verfügen.

4. **Richtige Antwort: B**
   A. **Falsch:** Die Richtlinie *Kennwortverwendung für Wechseldatenträger konfigurieren* ermöglicht die Konfiguration von Kennwortrichtlinien für Wechseldatenträger. Mit dieser Richtlinie können Sie nicht dafür sorgen, dass das BitLocker To Go-Lesetool auf allen FAT-formatierten Wechseldatenträgern verfügbar ist, die mit BitLocker geschützt werden.
   B. **Richtig:** Mit der Richtlinie *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen* können Sie dafür sorgen, dass das BitLocker To Go-Lesetool auf allen FAT-formatierten Wechseldatenträgern verfügbar ist, die mit BitLocker geschützt werden.
   C. **Falsch:** Die Richtlinie *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können* ermöglicht die Konfiguration der Wiederherstellungsoptionen für Wechseldatenträger. Mit dieser Richtlinie können Sie nicht dafür sorgen, dass das BitLocker To Go-Lesetool auf allen FAT-formatierten Wechseldatenträgern verfügbar ist, die mit BitLocker geschützt werden.
   D. **Falsch:** Die Richtlinie *Verwendung von BitLocker auf Wechseldatenträgern steuern* legt fest, ob sich BitLocker auf Wechseldatenträgern verwenden lässt. Mit dieser Richtlinie können Sie nicht dafür sorgen, dass das BitLocker To Go-Lesetool auf allen FAT-formatierten Wechseldatenträgern verfügbar ist, die mit BitLocker geschützt werden.

5. **Richtige Antwort: A**
   A. **Richtig:** Mit dem Befehlszeilenprogramm *Manage-bde.exe* können Sie den Wert im ID-Feld eines BitLocker-geschützten Volumes überprüfen.
   B. **Falsch:** Das Hilfsprogramm *Cipher.exe* ermöglicht die Verwaltung von EFS und nicht von BitLocker. Mit *Cipher.exe* können Sie nicht den Wert im ID-Feld eines BitLocker-geschützten Volumes überprüfen.
   C. **Falsch:** Das Hilfsprogramm *Bcdedit.exe* ermöglicht die Verwaltung der Startkonfiguration. Mit *Bcdedit.exe* können Sie nicht den Wert im ID-Feld eines BitLocker-geschützten Volumes überprüfen.
   D. **Falsch:** Das Hilfsprogramm *Sigverif.exe* ermöglicht die Überprüfung der digitalen Signaturen von Dateien. Mit *Sigverif.exe* können Sie nicht den Wert im ID-Feld eines BitLocker-geschützten Volumes überprüfen.

Lektion 2

1. **Richtige Antwort: C**
   A. **Falsch:** Der Befehl `Powercfg.exe -devicequery all_devices` listet alle Geräte auf. Er liefert keine Informationen darüber, welche Geräte so konfiguriert wurden, dass sie den Computer aus jedem Standbymodus reaktivieren können.

B. **Falsch:** Der Befehl `Powercfg.exe -hibernate` aktiviert den Ruhezustand. Mit ihm können Sie keine Liste der Geräte aufstellen, die so konfiguriert wurden, dass sie den Computer aus jedem Standbymodus reaktivieren können.

C. **Richtig:** Der Befehl `Powercfg.exe -devicequery wake_armed` zeigt eine Liste der Geräte eines Windows 7-Computers an, die so konfiguriert wurden, dass sie den Computer aus jedem Standbymodus reaktivieren können.

D. **Falsch:** Der Befehl `Powercfg.exe -list` zeigt eine Liste aller Energieschemas aus der aktuellen Umgebung des Benutzers an. Er zeigt keine Liste der Geräte an, die so konfiguriert wurden, dass sie den Computer aus jedem Standbymodus reaktivieren können.

2. **Richtige Antworten: A, B und C**

A. **Richtig:** Ein Benutzerkonto, das kein Mitglied der lokalen Gruppe *Administratoren* ist, kann dazu verwendet werden, einen anderen Energiesparplan auszuwählen.

B. **Richtig:** Ein Benutzerkonto, das kein Mitglied der lokalen Gruppe *Administratoren* ist, kann dazu verwendet werden, einen neuen Energiesparplan zu erstellen.

C. **Richtig:** Ein Benutzerkonto, das kein Mitglied der lokalen Gruppe *Administratoren* ist, kann dazu verwendet werden, die Netzschaltereinstellungen zu ändern.

D. **Falsch:** Ein Benutzerkonto, das kein Mitglied der lokalen Gruppe *Administratoren* ist, kann nicht zur Änderung der Einstellung *Kennwort bei Reaktivierung anfordern* verwendet werden.

3. **Richtige Antwort: C**

A. **Falsch:** Die Seite *Energieoptionen* der Systemsteuerung eignet sich nicht zur Übertragung eines benutzerdefinierten Energiesparplans von einem Windows 7-Computer auf einen anderen.

B. **Falsch:** Sie können die Einstellungen für Energiesparpläne zwar mit dem Editor für lokale Gruppenrichtlinien (*Gpedit.msc*) ändern, aber nicht auf andere Computer übertragen. Mit dem Editor für lokale Gruppenrichtlinien lassen sich nur sicherheitsbezogene Einstellungen übertragen.

C. **Richtig:** Mit *Powercfg.exe* können Sie einen Energiesparplan von einem Computer auf einen anderen übertragen.

D. **Falsch:** *Bcdedit.exe* dient zur Änderung der Startkonfiguration eines Computers. Das Programm eignet sich nicht zur Bearbeitung von Energiesparplänen.

4. **Richtige Antwort: B**

A. **Falsch:** Die Anmeldeinformationsverwaltung dient zur Verwaltung gespeicherter Anmeldeinformationen. Damit lassen sich keine Synchronisationskonflikte von Offlinedateien beheben.

B. **Richtig:** Synchronisationskonflikte von Offlinedateien lassen sich mit dem Synchronisierungscenter beheben.

C. **Falsch:** Die Seite *Heimnetzgruppe* der Systemsteuerung dient zur Verwaltung von Einstellungen für Heimnetzgruppen. Damit lassen sich keine Synchronisationskonflikte von Offlinedateien beheben.

D. **Falsch:** Das Netzwerk- und Freigabecenter eignet sich nicht zur Auflösung von Synchronisationskonflikten mit Offlinedateien. Es dient zur Verwaltung der Netzwerkkonfiguration.

5. **Richtige Antwort: D**

A. **Falsch:** Die Richtlinie *Übertragungsrate für langsame Verbindungen konfigurieren* ermöglicht die Festlegung eines Schwellenwerts für den Wechsel in den Modus für langsame Verbindungen. Der Modus für langsame Verbindungen ist für Offlinedateien vorgesehen. In der Frage heißt es aber, dass es nicht erforderlich ist, eine Datei offline verfügbar zu machen.

B. **Falsch:** Mit der Richtlinie *Modus für langsame Verbindungen konfigurieren* kann der Computer so eingestellt werden, dass er bei Bedarf den Modus für langsame Verbindungen verwendet. Das ist die Standardeinstellung für Windows 7-Clients. Der Modus für langsame Verbindungen ist für Offlinedateien vorgesehen. In der Frage heißt es aber, dass es nicht erforderlich ist, eine Datei offline verfügbar zu machen.

C. **Falsch:** Mit der Richtlinie *Dateien aus der Zwischenspeicherung ausschließen* lässt sich die Offlineverfügbarkeit bestimmter Dateitypen sperren. Diese Richtlinie eignet sich nicht dazu, einen Windows 7-Client für die Zwischenspeicherung von Dateien zu konfigurieren.

D. **Richtig:** Die transparente Zwischenspeicherung ermöglicht Windows 7 eine lokale Zwischenspeicherung von Dateien, wenn die Roundtrip-Netzwerklatenz zum Remotedateiserver einen vorgegebenen Schwellenwert (in Millisekunden) überschreitet.

Kapitel 11: Antworten zu den Übungen mit Fallbeispiel

Übung 1: Zugriff auf Offlinedateien bei Contoso

1. Sie exportieren den benutzerdefinierten Energiesparplan mit *Powercfg.exe* vom Referenzcomputer und importieren ihn auf den anderen Computern der Zweigstellen. Gruppenrichtlinien eignen sich nicht, weil die Computer keine Mitglieder einer AD DS-Domäne sind.
2. Sie aktivieren die transparente Zwischenspeicherung. BranchCache können Sie nicht verwenden, weil auf keinem der Dateiserver von Contoso das dafür erforderliche Betriebssystem Windows Server 2008 R2 installiert ist.
3. Synchronisationskonflikte mit Offlinedateien lassen sich mit dem Synchronisierungscenter lösen.

Übung 2: Verwenden von BitLocker bei Tailspin Toys

1. Um Benutzern von Windows XP oder Windows Vista den Zugriff auf USB-Speichergeräte zu ermöglichen, die mit BitLocker To Go verschlüsselt wurden, konfigurieren Sie die Richtlinie *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen*.
2. Sie können die Verwendung von Wechseldatenträgern mit Gruppenrichtlinien so einschränken, dass auf den Windows 7-Clients nur Geräte verwendbar sind, die mit BitLocker To Go geschützt sind und mit einer bestimmten Kennung versehen wurden.

Das erreichen Sie mit den Richtlinien *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind* und *Eindeutige IDs für Ihre Organisation angeben*.

3. Sie können für die Wechseldatenträger einen DRA konfigurieren und mit den entsprechenden Richtlinien dafür sorgen, dass Schlüssel und Kennwörter in AD DS gespeichert werden.

Kapitel 12: Antworten zur Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: B**
   A. **Falsch:** Die Deinstallation von Updates erfordert erhöhte Rechte und kann nicht mit einem Standardbenutzerkonto durchgeführt werden.
   B. **Richtig:** Die Standardeinstellungen von Windows Update unter Windows 7 erlauben einem Standardbenutzer die Installation von Updates.
   C. **Falsch:** Die Standardeinstellungen von Windows Update unter Windows 7 erlauben einem Standardbenutzer nicht, den Installationszeitpunkt von Updates zu ändern. Für diese Aufgabe sind erhöhte Rechte erforderlich.
   D. **Falsch:** Die Standardeinstellungen von Windows Update unter Windows 7 erlauben einem Standardbenutzer nicht, das Verhalten in Bezug auf das Herunterladen und Installieren von Updates zu ändern. Für diese Aufgabe sind erhöhte Rechte erforderlich.
   E. **Falsch:** Die Standardeinstellungen von Windows Update unter Windows 7 erlauben einem Standardbenutzer nicht, Updates auszublenden. Für diese Aufgabe sind erhöhte Rechte erforderlich.
2. **Richtige Antworten: B und C**
   A. **Falsch:** Sie sollten die Updateeinstellungen nicht ändern, damit andere wichtige Updates auch weiterhin auf den Windows 7-Clients installiert werden können.
   B. **Richtig:** Sie müssen das Update deinstallieren. Dadurch wird die benutzerdefinierte Anwendung wieder verwendungsfähig.
   C. **Richtig:** Sie sollten das Update nach seiner Deinstallation ausblenden. Wenn Sie das Update nicht ausblenden, wird es wieder für eine Installation verfügbar. Da Standardbenutzer standardmäßig Updates installieren können, würde dies wahrscheinlich zu einer erneuten Installation des problematischen Updates führen. Sobald die Lösung für die benutzerdefinierte Anwendung verfügbar wird, können Sie das Update wieder einblenden und anschließend installieren.
   D. **Falsch:** Sie dürfen das Update nicht installieren. Dadurch würden sich Probleme mit der benutzerdefinierten Anwendung ergeben.
3. **Richtige Antwort: C**
   A. **Falsch:** Sie sollten die Richtlinie *Erneut zu einem Neustart für geplante Installationen auffordern* nicht konfigurieren, weil sie festlegt, wie lange ein Benutzer einen anstehenden Neustart aufschieben kann. Sie stellt nicht sicher, dass geplante Updates, die nicht stattfanden, weil der Computer zu dem Zeitpunkt ausgeschaltet war, nach dem Einschalten des Computers nachgeholt werden.

B. **Falsch:** Sie sollten die Richtlinie *Neustart für geplante Installationen verzögern* nicht konfigurieren, weil sie festlegt, wie lange Windows nach einer geplanten Installation mit dem anstehenden Neustart wartet. Sie stellt nicht sicher, dass geplante Updates, die nicht stattfanden, weil der Computer zu dem Zeitpunkt ausgeschaltet war, nach dem Einschalten des Computers nachgeholt werden.

C. **Richtig:** Sie sollten die Richtlinie *Zeitplan für geplante Installationen neu erstellen* konfigurieren, weil der Computer dann geplante Installationen, die übersprungen wurden, weil der Computer zu dem Zeitpunkt ausgeschaltet war, nach dem nächsten Einschalten nachholen kann.

D. **Falsch:** Sie sollten die Richtlinie *Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind* nicht konfigurieren, weil sie einem Benutzer ermöglicht, angemeldet zu bleiben, obwohl nach einer Installation eigentlich ein Neustart erforderlich ist. Sie stellt nicht sicher, dass geplante Updates, die nicht stattfanden, weil der Computer zu dem Zeitpunkt ausgeschaltet war, nach dem Einschalten des Computers nachgeholt werden.

4. **Richtige Antwort: D**

A. **Falsch:** Sie sollten die Richtlinie *Softwarebenachrichtigungen aktivieren* nicht konfigurieren. Diese Richtlinie steuert die Benachrichtigung der Benutzer über verfügbare Updates. Sie eignet sich nicht, um Windows Update auf die Verwendung eines WSUS-Servers statt der Microsoft Update-Server einzustellen.

B. **Falsch:** Sie sollten die Richtlinie *Suchhäufigkeit für automatische Updates* nicht konfigurieren. Diese Richtlinie legt fest, wie oft Windows Update überprüft, ob neue Updates vorliegen. Sie eignet sich nicht, um Windows Update auf die Verwendung eines WSUS-Servers statt der Microsoft Update-Server einzustellen.

C. **Falsch:** Sie sollten die Richtlinie *Automatische Updates konfigurieren* nicht konfigurieren. Diese Richtlinie legt fest, welche Updates installiert werden sollen und ob sie heruntergeladen und installiert werden oder ob der angemeldete Benutzer informiert werden soll. Sie eignet sich nicht, um Windows Update auf die Verwendung eines WSUS-Servers statt der Microsoft Update-Server einzustellen.

D. **Richtig:** Sie sollten die Richtlinie *Internen Pfad für den Microsoft Updatedienst angeben* konfigurieren, weil Sie mit ihr einen lokalen WSUS-Server als Updatequelle angeben können.

5. **Richtige Antwort: D**

A. **Falsch:** Microsoft Update erstellt keine Übersichtsberichte, aus denen hervorgeht, auf welchen Clients einer Organisation bestimmte Updates fehlen. Microsoft Update dient in Organisationen, die keine Lösungen wie WSUS, System Center Essentials 2007 oder SCCM 2007 verwenden, als Updatequelle.

B. **Falsch:** Da in Ihrer Organisation kein WSUS-Server bereitgestellt wird, können Sie auch nicht mit einem WSUS-Server überprüfen, welche Updates fehlen.

C. **Falsch:** Mit der Konsole *Gruppenrichtlinienverwaltung* können Sie nicht überprüfen, ob Updates fehlen. Die Konsole *Gruppenrichtlinienverwaltung* dient in einer Domänenumgebung zur Verwaltung der Gruppenrichtlinien.

D. **Richtig:** Mit MBSA können Sie die Computer auf fehlende Softwareupdates überprüfen, auf denen Sie über Administratorrechte verfügen.

Lektion 2

1. **Richtige Antwort: D**
   A. **Falsch:** Sie sollten die Sicherheitsstufe der Zone *Intranet* nicht ändern. Die Sicherheitsstufe steuert, wie der Internet Explorer mit Downloads und Cookies umgeht. Wenn Sie diese Einstellung konfigurieren, vertraut der Internet Explorer nicht der Zertifizierungsstelle, die das Zertifikat für *timesheet.contoso.internal* ausgestellt hat.
   B. **Falsch:** Wenn Sie den Popupblocker deaktivieren, werden Popups erlaubt. So veranlassen Sie den Internet Explorer nicht, dem Websitezertifikat zu vertrauen.
   C. **Falsch:** Wenn Sie die Website im InPrivate-Modus besuchen, bedeutet das nicht, dass der Internet Explorer dem Zertifikat vertraut, das für die Website ausgestellt wurde. Wenn Sie den InPrivate-Modus verwenden, zeichnet der Internet Explorer keine Daten zur Browsernavigation auf.
   D. **Richtig:** Weil das Zertifikat der Website von einer internen Zertifizierungsstelle ausgestellt wurde und Sie nicht direkt für das Unternehmen arbeiten, wurde der Internet Explorer nicht so konfiguriert, dass er der internen Zertifizierungsstelle vertraut. Um die interne Zertifizierungsstelle als vertrauenswürdig einzustufen, müssen Sie ihre Website besuchen und das Zertifikat der Zertifizierungsstelle herunterladen und installieren.
2. **Richtige Antworten: A und B**
   A. **Richtig:** Um sicherzustellen, dass Benutzer nicht versehentlich die Standardschnellinfo *Mit Windows Live bloggen* verwenden, sollten Sie sie deaktivieren.
   B. **Richtig:** Um sicherzustellen, dass die Benutzer die selbstentwickelte Blogschnellinfo verwenden können, müssen Sie sie installieren.
   C. **Falsch:** Sie sollten die Schnellinfo *Mit Windows Live bloggen* nicht zur Standardschnellinfo für die Rubrik *Bloggen* im Internet Explorer machen. Weil Sie verhindern wollen, dass die Benutzer diese Schnellinfo versehentlich verwenden, sollten Sie sie deaktivieren.
   D. **Falsch:** Sie sollten die selbstentwickelte Blogschnellinfo nicht deaktivieren, weil die Benutzer diese Schnellinfo verwenden sollen, um auf der Intranetsite zu bloggen.
3. **Richtige Antworten: A und C**
   A. **Richtig:** Sie sollten die Site *www.wingtiptoys.com* als Ausnahme eintragen, damit Popupfenster dieser Site vom Internet Explorer angezeigt werden.
   B. **Falsch:** Sie sollten die Blockierungsebene nicht auf *Mittel* setzen, weil dann Popups von anderen Sites als denen in der Ausnahmenliste zugelassen werden.
   C. **Richtig:** Sie sollten die Blockierungsebene auf *Hoch* setzen, weil dadurch alle Popupfenster außer denen von Sites in der Ausnahmenliste blockiert werden.
   D. **Falsch:** Sie sollten die Blockierungsebene nicht auf *Niedrig* setzen, weil dann Popups von anderen Sites als denen in der Ausnahmenliste zugelassen werden.

4. **Richtige Antwort: D**
   A. **Falsch:** Das Problem hat nichts mit InPrivate-Browsen zu tun. Es hat mit der Kompatibilitätsansicht zu tun, was Sie daran sehen, dass die Websites auf Windows XP- und Windows Vista-Clients einwandfrei im Internet Explorer dargestellt werden. Windows XP- und Windows Vista-Clients können zwar auch den Internet Explorer 8 ausführen, der Hinweis deutet aber darauf hin, dass es sich um ein Kompatibilitätsproblem handelt.
   B. **Falsch:** Das Problem hat nichts mit InPrivate-Filterung zu tun. Es hat mit der Kompatibilitätsansicht zu tun, was Sie daran sehen, dass die Websites auf Windows XP- und Windows Vista-Clients einwandfrei im Internet Explorer dargestellt werden. Windows XP- und Windows Vista-Clients können zwar auch den Internet Explorer 8 ausführen, der Hinweis deutet aber darauf hin, dass es sich um ein Kompatibilitätsproblem handelt.
   C. **Falsch:** In der Frage wird darauf hingewiesen, dass die Websites auf Windows XP- und Windows Vista-Clients einwandfrei im Internet Explorer angezeigt werden. Windows XP- und Windows Vista-Clients können zwar auch den Internet Explorer 8 ausführen, der Hinweis deutet aber darauf hin, dass es sich um ein Kompatibilitätsproblem handelt. Das Problem wird nicht dadurch gelöst, dass Sie die Kompatibilitätsansicht deaktivieren.
   D. **Richtig:** Sie sollten die Liste der Intranetsites, die nicht richtig dargestellt werden, über die Richtlinie *Richtlinienliste von Internet Explorer 7-Sites verwenden* konfigurieren. Der Internet Explorer zeigt diese Sites dann in der Kompatibilitätsansicht an.
5. **Richtige Antwort: B**
   A. **Falsch:** Wenn Sie eine InPrivate-Browsen-Sitzung starten, hindert das fremde Websites nicht daran, Ihre Aktivitäten zu verfolgen, wenn sie Inhalte für mehrere Sites zuliefern, die Sie besuchen. InPrivate-Browsen-Sitzungen nehmen trotzdem Cookies an und übertragen Daten.
   B. **Richtig:** Wenn Sie die InPrivate-Filterung aktivieren, findet und blockiert der Internet Explorer Inhalte von Websites, die während einer Browsersitzung auf mehreren anderen Sites auftauchen.
   C. **Falsch:** Wenn Sie den Popupblocker deaktivieren, hindert das fremde Websites nicht daran, Ihre Aktivitäten zu verfolgen, wenn sie Inhalte für mehrere Sites zuliefern, die Sie besuchen. Wenn Sie den Popupblocker deaktivieren, bekommen Sie Popupwebseiten angezeigt, die normalerweise blockiert würden.
   D. **Falsch:** Sie sollten den SmartScreen-Filter nicht deaktivieren. Er schützt Sie vor Phishing-Angriffen. Wenn Sie den SmartScreen-Filter deaktivieren, warnt der Internet Explorer Sie nicht mehr, wenn Sie eine Website besuchen, die böswillige Software enthält oder im Verdacht steht, Phishing zu betreiben.

Kapitel 12: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Windows Update bei Contoso

1. Sie sollten für die Computer in der Niederlassung Canberra die Richtlinie *Internen Pfad für den Microsoft Updatedienst angeben* konfigurieren. Mit dieser Richtlinie können Sie die Adresse des lokalen WSUS-Servers angeben.
2. Sie sollten die Richtlinie *Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivieren* konfigurieren. Wenn diese Richtlinie auf kompatiblen Computern konfiguriert ist, wachen sie zur festgelegten Uhrzeit auf und spielen die Updates ein.
3. Melden Sie sich über den Remotedesktop an jedem Computer in den Niederlassungen Brisbane und Adelaide an. Deinstallieren Sie das Update und blenden Sie es aus. So ist sichergestellt, dass dieses Update nicht erneut automatisch installiert wird.

Übung mit Fallbeispiel 2: Internet Explorer bei Wingtip Toys

1. Sie können die Verwendung von Internet Explorer-Schnellinfos mithilfe von Gruppenrichtlinien deaktivieren. Es ist zwar auch möglich, die Schnellinfos von Hand zu deaktivieren, aber wenn Sie das nicht über Gruppenrichtlinien erledigen, können die Benutzer die gelöschten oder andere Schnellinfos von Hand erneut installieren.
2. Empfehlen Sie ihnen, die InPrivate-Filterung zu aktivieren. Die InPrivate-Filterung verhindert, dass Browsersitzungen über mehrere Sites hinweg verfolgt werden. Beim InPrivate-Browsen wird dagegen nicht verhindert, dass Browsersitzungen über mehrere Sites hinweg verfolgt werden; es verhindert lediglich, dass der Internet Explorer den Browserverlauf und andere Daten aufzeichnet.
3. Fügen Sie die Sites zur Liste der Sites hinzu, die in der Kompatibilitätsansicht dargestellt werden. Dazu können Sie entweder das Dialogfeld *Einstellungen der Kompatibilitätsansicht* verwenden oder die Liste mithilfe von Gruppenrichtlinien verteilen.

Kapitel 13: Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: A**
   A. **Richtig:** Die schlechteste Teilbewertung bestimmt die Gesamtbewertung, selbst wenn dieser Computer nicht in erster Linie für 3D-Grafik und Spiele eingesetzt wird.
   B. **Falsch:** 3,9 ist der Durchschnittswert der Teilbewertungen. Aber die schlechteste Teilbewertung bestimmt die Gesamtbewertung, nicht der Durchschnitt.
   C. **Falsch:** 5,1 ist ein wichtiger Wert, weil der Computer für prozessorintensive Operationen benutzt wird. Die Frage war aber, wie der Windows-Leistungsindex des Computers lautet, und die schlechteste Teilbewertung bestimmt die Gesamtbewertung.
   D. **Falsch:** 5,3 ist die beste Teilbewertung. Die schlechteste Teilbewertung bestimmt die Gesamtbewertung, nicht die höchste.

2. **Richtige Antwort: A**
   A. **Richtig:** Die Zuverlässigkeitsüberwachung überwacht Anwendungsinstallationen. Sie können damit feststellen, welche Anwendungen wann installiert wurden.
   B. **Falsch:** Das Wartungscenter verrät Ihnen, wenn eine Anwendung oder ein Gerätetreiber nicht richtig funktioniert. Sie können darin nicht feststellen, wann eine Anwendung installiert wurde.
   C. **Falsch:** Sammlungssätze zeichnen aktuelle Leistungs- und Konfigurationsdaten auf. Sie verraten Ihnen nicht, wann eine Anwendung installiert wurde.
   D. **Falsch:** In der Leistungsüberwachung können Sie sich Leistungsindikatoren in Echtzeit ansehen oder Leistungsdaten aus einem Sammlungssatz analysieren. Die Leistungsüberwachung zeichnet aber nicht auf, wann eine Anwendung installiert wurde.
3. **Richtige Antworten: A, B, C und E**
   A. **Richtig:** Anwendungsabstürze werden in der Zuverlässigkeitsüberwachung aufgezeichnet.
   B. **Richtig:** Windows-Fehler werden in der Zuverlässigkeitsüberwachung aufgezeichnet.
   C. **Richtig:** Anwendungsinstallationen und -deinstallationen werden in der Zuverlässigkeitsüberwachung aufgezeichnet.
   D. **Falsch:** Wenn ein Dienst gestartet oder beendet wird, wird das normalerweise im Ereignisprotokoll aufgezeichnet, aber nicht in der Zuverlässigkeitsüberwachung.
   E. **Richtig:** Gerätetreiberfehler werden in der Zuverlässigkeitsüberwachung aufgezeichnet.
4. **Richtige Antwort: A**
   A. **Richtig:** Mit dem Tool Wecutil konfigurieren Sie den Ereignissammlungsdienst.
   B. **Falsch:** Der Befehl `winrm` konfiguriert WinRM. Normalerweise führen Sie ihn auf einem Quellcomputer aus. Sie können ihn auch auf dem Sammelcomputer ausführen, wenn Sie ein quellinitiiertes Abonnement konfigurieren, aber das ist im beschriebenen Szenario nicht wichtig, weil *Canberra* Ereignisse von *Aberdeen* ausliest. Ohnehin konfiguriert dieser Befehl nicht den Ereignissammlungsdienst.
   C. **Falsch:** Der Befehl `winrm` konfiguriert WinRM. Hier führen Sie ihn im automatischen Modus aus. Unabhängig davon, ob Sie das Argument `-q` angeben oder nicht, konfiguriert dieser Befehl nicht den Ereignissammlungsdienst.
   D. **Falsch:** Dieser Befehl startet den Gruppenrichtlinien-Editor. Sie können mithilfe von Gruppenrichtlinien Quellcomputer zu einem quellinitiierten Abonnement hinzufügen, aber das ist im beschriebenen Szenario nicht wichtig. Dieser Befehl konfiguriert nicht den Ereignissammlungsdienst.
5. **Richtige Antwort: B**
   A. **Falsch:** Auf der Registerkarte *Allgemein* stellen Sie ein, wie oft das Diagramm aktualisiert wird und wie viele Daten angezeigt werden, bevor die Leistungsüberwachung das Diagramm von der linken Seite her überschreibt. Außerdem können Sie wählen, ob die Legende, die Wertleiste und die Symbolleiste angezeigt werden und ob die Berichts- und Histogrammsansicht Standard-, Maximal-, Minimal-,

Durchschnitts- oder aktuelle Werte anzeigen. Sie können hier nicht einstellen, ob die aktuelle Aktivität in Echtzeit oder Protokolldateien angezeigt werden, die mit einem Sammlungssatz gespeichert wurden.

B. **Richtig:** Auf der Registerkarte *Quelle* wählen Sie aus, ob die aktuelle Aktivität in Echtzeit oder Protokolldateien angezeigt werden, die mit einem Sammlungssatz gespeichert wurden. Wenn Sie eine Protokolldatei anzeigen, können Sie auf dieser Registerkarte außerdem festlegen, welcher Zeitbereich im Leistungsüberwachungsfenster angezeigt wird.

C. **Falsch:** Auf der Registerkarte *Daten* konfigurieren Sie die Anzeige der einzelnen Leistungsindikatoren. Wählen Sie in der Liste *Leistungsindikatoren* aus, welchen Leistungsindikator Sie konfigurieren wollen, und passen Sie Farbe, Breite und Stil an. Sie können außerdem die Skalierung vergrößern oder verkleinern. Sie können hier nicht einstellen, ob die aktuelle Aktivität in Echtzeit oder Protokolldateien angezeigt werden, die mit einem Sammlungssatz gespeichert wurden.

D. **Falsch:** Auf der Registerkarte *Grafik* wählen Sie aus, ob für die Anzeige des Diagramms ein Bildlauf durchgeführt wird und welcher Diagrammtyp verwendet wird. Sie können hier nicht einstellen, ob die aktuelle Aktivität in Echtzeit oder Protokolldateien angezeigt werden, die mit einem Sammlungssatz gespeichert wurden.

E. **Falsch:** Wenn Sie mehrere Systemmonitorfenster gleichzeitig öffnen, können Sie auf der Registerkarte *Darstellung* die Farbe des Hintergrunds oder anderer Elemente ändern. So ist es einfacher, die Fenster zu unterscheiden. Sie können hier nicht einstellen, ob die aktuelle Aktivität in Echtzeit oder Protokolldateien angezeigt werden, die mit einem Sammlungssatz gespeichert wurden.

Lektion 2

1. **Richtige Antwort: D**

   A. **Falsch:** Im WMI CIM Studio können Sie Klassen, Eigenschaften, Kennzeichner und Instanzen aus einem CIM-Repository ansehen und bearbeiten, ausgewählte Methoden ausführen und MOF-Dateien generieren und kompilieren. Sie können sich damit keine von der Windows-Verwaltung generierten Ereignisse und Ereignisinformationen wie Datum und Uhrzeit, Klasse, Ursprung und Beschreibung ansehen.

   B. **Falsch:** Im WMI Object Browser können Sie Objekte ansehen, Eigenschaftswerte und Kennzeichner ändern und Methoden ausführen. Sie können sich damit keine von der Windows-Verwaltung generierten Ereignisse und Ereignisinformationen wie Datum und Uhrzeit, Klasse, Ursprung und Beschreibung ansehen.

   C. **Falsch:** Im WMI Event Registration Tool können Sie ständige Ereignisempfänger konfigurieren und Instanzen von Ereignisempfänger-, Filter-, Bindungs- und Zeitgebersystemklassen anlegen oder ansehen. Sie können sich damit keine von der Windows-Verwaltung generierten Ereignisse und Ereignisinformationen wie Datum und Uhrzeit, Klasse, Ursprung und Beschreibung ansehen.

D. **Richtig:** Der WMI Event Viewer zeigt Ereignisse aller Instanzen von registrierten Verbrauchern an. Sie können sich damit die von der Windows-Verwaltung generierten Ereignisse und Ereignisinformationen wie Datum und Uhrzeit, Klasse, Ursprung und Beschreibung ansehen.

2. **Richtige Antwort: C**
   A. **Falsch:** Das Performance Analyzer Tool (*Xperfview.exe*) kann aufgezeichnete Ablaufverfolgungen anzeigen. Es zeichnet keine Abbilder auf.
   B. **Falsch:** Das On/Off Transition Trace Capture Tool (*Xbootmgr.exe*) sammelt Informationen während der An-/Aus-Umschaltphasen von Windows 7. Es zeichnet keine Benutzer und Kernelablaufverfolgungen auf und führt keine Ablaufverfolgungen zusammen.
   C. **Richtig:** Das Trace Capture, Processing, and Command-Line Analysis Tool (*Xperf.exe*) zeichnet Benutzer und Kernelablaufverfolgungen auf und führt sie in einer einzigen Ablaufverfolgung zusammen.
   D. **Falsch:** Visual Trace Analyse ist ein anderer Name für das Performance Analyzer Tool (*Xperfview.exe*). Es zeigt aufgezeichnete Abbilder an, zeichnet aber keine Abbilder auf.
3. **Richtige Antwort: B**
   A. **Falsch:** Der Process Explorer hilft Ihnen festzustellen, welche Anwendungen für Aktivitäten auf Ihrer Festplatte verantwortlich sind und auf welche Dateien und Ordner zugegriffen wird. Dieses Tool müssen Sie aber gesondert herunterladen, es ist nicht in Windows 7 enthalten.
   B. **Richtig:** Das Tool *Ressourcenmonitor* ist in Windows 7 enthalten. Es hilft Ihnen festzustellen, welche Anwendungen für Aktivitäten auf Ihrer Festplatte verantwortlich sind und auf welche Dateien und Ordner zugegriffen wird.
   C. **Falsch:** Der Task-Manager verrät Ihnen, welche Anwendungen, Dienste und Prozesse auf Ihrem Computer laufen. Er liefert Systemdetails, zum Beispiel die Zahl der benutzten Handles und Threads, und gibt die aktuelle Prozessorauslastung an. Er hilft Ihnen aber nicht festzustellen, welche Anwendungen für Aktivitäten auf Ihrer Festplatte verantwortlich sind.
   D. **Falsch:** Der Windows-Leistungsindex misst die Fähigkeit Ihres Computers, ressourcenintensive Anwendungen wie Spiele und Grafikprogramme auszuführen. Er hilft Ihnen aber nicht festzustellen, welche Anwendungen für Aktivitäten auf Ihrer Festplatte verantwortlich sind.
4. **Richtige Antwort: A**
   A. **Richtig:** Die Prozesszugehörigkeit legt fest, ob ein Prozess einen bestimmten Prozessor benutzt oder immer den Prozessor verwendet, der am wenigsten zu tun hat. Angesichts der beschriebenen Symptome sind mehrere wichtige Prozesse an den ursprünglichen Prozessor gebunden und müssen so konfiguriert werden, dass sie auch den zweiten Prozessor verwenden können. Sie konfigurieren die Prozesszugehörigkeit im Task-Manager.
   B. **Falsch:** Die Prozesspriorität legt fest, wie schnell ein Prozess ausgeführt wird und welchen Zugriff er im Vergleich mit anderen Prozessen auf wichtige Ressourcen hat. Sie legt nicht fest, welche Prozessoren der Prozess benutzen darf.

C. **Falsch:** Sie können im Tool *Leistungsoptionen* die optimalen Leistungseinstellungen für Programme oder Hintergrunddienste wählen. Auf einem Clientcomputer verwenden Sie normalerweise die Option *Programme*. Das hat aber keine Auswirkung darauf, welchen Prozessor ein laufender Prozess benutzen darf.

D. **Falsch:** Einstellungen für virtuellen Arbeitsspeicher legen fest, wie viel Festplattenplatz als ausgelagerter Arbeitsspeicher genutzt wird. Das hat keine Auswirkung darauf, welchen Prozessor ein laufender Prozess benutzen darf.

5. **Richtige Antwort: D**

A. **Falsch:** Die Konsole *Dienste* listet alle Dienste auf, die auf einem Computer verfügbar sind, liefert Informationen über jeden Dienst und stellt Optionen für die Dienstverwaltung bereit. Unter anderem sehen Sie in der Konsole *Dienste* den Starttyp und die Anmeldedaten eines Dienstes. Sie können in dieser Konsole nicht festlegen, welches Betriebssystem in einer Dual-Boot-Konfiguration standardmäßig gestartet wird oder wie Windows 7 bei einem Systemfehler reagiert.

B. **Falsch:** Mit dem Tool *Leistungsoptionen* können Sie visuelle Effekte konfigurieren, die Leistung für Anwendungen oder Hintergrunddienste optimieren und DEP-Einstellungen konfigurieren. Sie können damit nicht festlegen, welches Betriebssystem in einer Dual-Boot-Konfiguration standardmäßig gestartet wird oder wie Windows 7 bei einem Systemfehler reagiert.

C. **Falsch:** Der Task-Manager liefert Daten zur aktuellen Ressourcennutzung. Außerdem können Sie damit abgestürzte Anwendungen beenden, Dienste beeden und starten oder die Prozesspriorität und -zugehörigkeit festlegen. Sie können mit nicht festlegen, welches Betriebssystem in einer Dual-Boot-Konfiguration standardmäßig gestartet wird oder wie Windows 7 bei einem Systemfehler reagiert.

D. **Richtig:** Mit dem Tool *Systemkonfiguration* (Msconfig) können Sie festlegen, welches Betriebssystem in einer Dual-Boot-Konfiguration standardmäßig gestartet wird oder wie Windows 7 bei einem Systemfehler reagiert.

Kapitel 13: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Verwenden von Sammlungssätzen und Ereignisweiterleitung

1. James zeichnet mit Sammlungssätzen eine Leistungsbaseline auf, während der Server normal arbeitet. Dann führt er dieselben Sammlungssätze von Hand aus, sobald das Leistungsproblem auftritt. Tauchen die Leistungsprobleme meist zu einer bestimmten Tageszeit auf, kann er die Leistungsdatensammelsätze so konfigurieren, dass sie über einen längeren Zeitraum hinweg Daten während dieser Uhrzeit aufzeichnen. Er analysiert die Ergebnisse in der Leistungsüberwachung, vergleicht die Daten mit seiner Baseline und ermittelt, welche Faktoren für die Probleme verantwortlich sein könnten.
2. James greift über den Remotedesktop auf den Server zu und führt die Zuverlässigkeitsüberwachung aus. Das zeigt ihm, welche Anwendungen auf dem Server zu dem Zeitpunkt installiert oder aktualisiert wurden, als die Probleme begannen.
3. James verwendet die Ereignisweiterleitung, um Ereignisse über knappen Festplattenplatz an einen zentralen Server weiterzuleiten. Nun kann er dieses Ereignisprotokoll

überwachen und Computer erkennen, denen der Festplattenplatz ausgeht. Außerdem kann er eine Aufgabe hinzufügen, die ihm automatisch mitteilt, dass ein Ereignis protokolliert wurde, das über knappen Festplattenplatz informiert.

Übung mit Fallbeispiel 2: Problembehandlung für Leistungsprobleme auf einem Clientcomputer

1. James muss die Zugehörigkeit der Prozesse auf dem Computer festlegen, vor allem bei denen, die den Prozessor stark auslasten. Vermutlich sind diese Prozesse so konfiguriert, dass sie nur den ursprünglichen Prozessor verwenden. James hat bereits den Task-Manager geöffnet, und in diesem Tool muss er auch die Prozesszugehörigkeit konfigurieren.
2. James klickt in der Systemsteuerung auf *Leistungsinformationen und -tools*, dann auf *Weitere Tools* und schließlich auf *Leistungsdetails im Ereignisprotokoll anzeigen*. Daraufhin öffnet sich die Ereignisanzeige, die alle Ereignisse aus dem Container *Betriebsbereit* unter *Diagnostics-Performance* anzeigt. Hier findet er wahrscheinlich Ereignisse, die mit Leistungsproblemen zu tun haben.
3. James sollte auf der Registerkarte *Richtlinien* im Eigenschaftendialogfeld des USB-Geräts die Option *Schnelles Entfernen* auswählen. Die Datenübertragung zwischen dem Computer und dem USB-Gerät ist dann zwar unter Umständen etwas langsamer, aber wenn das Flashlaufwerk versehentlich (oder absichtlich) abgezogen wird, ist die Gefahr viel geringer, dass die geschriebenen Daten verloren gehen.

Kapitel 14: Lernzielkontrolle

Lektion 1

1. **Richtige Antwort: C**
   A. **Falsch:** Das verstößt gegen die Unternehmensrichtlinie, die vorschreibt, dass Windows auswählt, welche Dateien und Ordner gesichert werden. Außerdem wird nicht erwähnt, dass der Benutzer ein lokaler Administrator oder ein Sicherungs-Operator auf seinem Computer ist; daher hat er wahrscheinlich nicht die Berechtigungen, die nötig sind, um die Sicherungseinstellungen zu ändern.
   B. **Falsch:** Wenn der Benutzer das Datensicherungsziel ändert, hat das keine Auswirkungen darauf, welche Dateien und Ordner gesichert werden. Außerdem hat der Benutzer wahrscheinlich nicht die erforderlichen Berechtigungen für diese Aufgabe.
   C. **Richtig:** Wenn Windows auswählt, welche Dateien gesichert werden, sichert es immer die Bibliothek *Dokumente*.
   D. **Falsch:** Wenn der Benutzer sofort eine Datensicherung ausführt, hat das keine Auswirkungen darauf, welche Dateien und Ordner gesichert werden. Außerdem hat der Benutzer wahrscheinlich nicht die erforderlichen Berechtigungen für diese Aufgabe.

2. **Richtige Antwort: D**
   A. **Falsch:** Die Datei wurde am Tag vor der nächtlichen Datensicherung erstellt und gelöscht, sie wurde also nicht gesichert.
   B. **Falsch:** Der Papierkorb wird während einer Datei- und Ordnersicherung nicht gesichert.
   C. **Falsch:** Die Datei wurde am vorherigen Tag erstellt und gelöscht, bevor sie gesichert werden konnte. Selbst wenn sich also eine Datei mit demselben Namen in einer älteren Datensicherung findet, ist es nicht die gesuchte.
   D. **Richtig:** Die nächtliche Datensicherung ändert nicht den Inhalt des Papierkorbs. Die Datei wurde am Abend zuvor gelöscht, daher befindet sie sich noch im Papierkorb.
3. **Richtige Antworten: A, B, C und D**
   A. **Richtig:** Dons Word- und Excel-Dateien aus seiner Bibliothek *Dokumente* werden standardmäßig gesichert. Don braucht dazu nicht am Computer angemeldet zu sein.
   B. **Richtig:** Kims Word- und Excel-Dateien aus ihrer Bibliothek *Dokumente* werden standardmäßig gesichert.
   C. **Richtig:** Dons Ordner Presentations befindet sich in seiner Bibliothek *Dokumente*, daher wird er standardmäßig gesichert.
   D. **Richtig:** Dons Bibliothek *Bilder* wird standardmäßig gesichert.
   E. **Falsch:** Verschlüsselte Dateien und Ordner werden nicht gesichert (selbst wenn sie sich in einer *Dokumente*-Bibliothek befinden).
   F. **Falsch:** Dateien im Papierkorb werden nicht gesichert.
   G. **Falsch:** In der Standardeinstellung ist ein USB-Flashstick mit dem Dateisystem FAT formatiert. Dateien auf einem solchen Gerät werden nicht gesichert.
4. **Richtige Antworten: A, B und E**
   A. **Richtig:** Sie können mit der Konsole *Sichern und Wiederherstellen* eine Systemabbildsicherung auf eine interne Festplatte schreiben.
   B. **Richtig:** Sie können mit der Konsole *Sichern und Wiederherstellen* eine Systemabbildsicherung auf eine externe Festplatte schreiben (sofern sie mit dem Dateisystem NTFS formatiert ist).
   C. **Falsch:** Sie können mit der Konsole *Sichern und Wiederherstellen* keine Systemabbildsicherung auf ein 8 GByte großes USB-Flashlaufwerk schreiben. Ein solches Medium können Sie allerdings für die Datei- und Ordnersicherungen einsetzen.
   D. **Falsch:** Sie können mit der Konsole *Sichern und Wiederherstellen* keine Systemabbildsicherung auf optische Datenträger schreiben. Solche Medien können Sie allerdings für die Datei- und Ordnersicherungen einsetzen.
   E. **Richtig:** Sie können mit der Konsole *Sichern und Wiederherstellen* eine Systemabbildsicherung in eine Netzwerkfreigabe schreiben, sofern der Computer unter Windows 7 Professional, Ultimate oder Enterprise läuft.

5. **Richtige Antwort: D**
   A. **Falsch:** Computer mit Windows 7 Ultimate bieten alle Windows 7-Features. Sie sind aber nicht die einzigen Windows 7-Computer, die in eine Netzwerkfreigabe gesichert werden können.
   B. **Falsch:** Computer mit Windows 7 Enterprise werden mit einer Volumenlizenz installiert und in einer Unternehmensumgebung meist in großer Zahl eingesetzt. Sie sind aber nicht die einzigen Windows 7-Computer, die in eine Netzwerkfreigabe gesichert werden können.
   C. **Falsch:** Manche Features, darunter das Starten von einer VHD, setzen Windows 7 Ultimate oder Enterprise voraus. Die Fähigkeit, eine Datensicherung in eine Netzwerkfreigabe zu schreiben, gehört aber nicht dazu.
   D. **Richtig:** Sie können Datensicherungen bei Computern mit Windows 7 Professional, Ultimate und Enterprise in eine Netzwerkfreigabe schreiben.

Lektion 2

1. **Richtige Antworten: A, C und D**
   A. **Richtig:** Im abgesicherten Modus werden nur wenige unverzichtbare Treiber geladen. Der Computer startet daraufhin erfolgreich, und Sie können die funktionierende Vorversion des unsignierten Treibers wiederherstellen.
   B. **Falsch:** Wenn Sie die Startprotokollierung aktivieren, wird eine Datei namens *Ntbtlog.txt* angelegt, die alle Treiber auflistet, die während des Systemstarts geladen werden. Darin ist auch zu erkennen, welche Datei zuletzt geladen wurde, bevor ein Fehler auftrat. In diesem Fall hilft Ihnen das nicht weiter, weil Sie das System starten wollen, ohne den problematischen Treiber zu laden.
   C. **Richtig:** Die Option *Anzeige mit niedriger Auflösung aktivieren (640x480)* lädt den Standardtreiber für die Anzeige, der nur eine geringe Auflösung bietet. Der problematische Treiber wird nicht geladen, sodass Sie den Computer starten und die Vorversion des Treibers wiederherstellen können.
   D. **Richtig:** Sie haben sich nicht angemeldet, seit der problematische Treiber installiert wurde. Die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* lädt den vorher installierten Treiber. In diesem Fall ist das die beste Lösung, weil sie den geringsten Aufwand erfordert.
   E. **Falsch:** Wenn Sie die Option *Erzwingen der Treibersignatur deaktivieren* wählen, ist es möglich, unsignierte Treiber zu installieren. Vermutlich haben Sie den Computer bereits entsprechend konfiguriert. Diese Option ermöglicht Ihnen nicht, die Vorversion des problematischen Treibers wiederherzustellen.
2. **Richtige Antworten: A und E**
   A. **Richtig:** Sie können den Computerschutz für interne Festplatten aktivieren, die üblicherweise mit NTFS formatiert sind.
   B. **Falsch:** Sie können den Computerschutz für externe Festplatten aktivieren, aber nur wenn sie mit NTFS formatiert sind.
   C. **Falsch:** Sie können den Computerschutz nicht für USB-Flashlaufwerke aktivieren.

D. **Falsch:** Sie können den Computerschutz nicht für optische Laufwerke aktivieren.

E. **Richtig:** Der Computerschutz kann für bereitgestellte VHDs aktiviert werden.

3. **Richtige Antwort: D**

A. **Falsch:** Sie können eine Systemwiederherstellung rückgängig machen, wenn Sie sie nach einem Start mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* durchgeführt haben. Dagegen können Sie eine Systemwiederherstellung nicht rückgängig machen, wenn sie mit den Systemwiederherstellungstools gestartet wurde.

B. **Falsch:** Sie können eine Systemwiederherstellung rückgängig machen, die Sie nach einem normalen Start oder einem Start mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* ausgeführt haben.

C. **Falsch:** Im geschilderten Fall können Sie die Systemwiederherstellung rückgängig machen, weil sie nach einem Start mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* durchgeführt wurde. Es ist aber falsch zu behaupten, dass Sie eine Systemwiederherstellung immer rückgängig machen können, unabhängig davon, wie Sie den Computer gestartet oder die Wiederherstellung eingeleitet haben.

D. **Richtig:** Wenn Sie eine Systemwiederherstellung nach einem normalen Start oder einem Start mit der Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* ausführen, wird ein Wiederherstellungspunkt erstellt, sodass Sie die Systemwiederherstellung rückgängig machen können.

4. **Richtige Antwort: A**

A. **Richtig:** Die Windows-Speicherdiagnose analysiert den Arbeitsspeicher (RAM) des Computers auf Hardwareprobleme.

B. **Falsch:** Die Systemstartreparatur behebt automatisch Probleme, die verhindern, dass Windows startet. Es ist unwahrscheinlich, dass Sie damit Hardwareprobleme im RAM diagnostizieren.

C. **Falsch:** Die Systemwiederherstellung stellt Systemdateien und -einstellungen aus dem letzten Wiederherstellungspunkt wieder her. Sie wird benutzt, wenn eine Änderung am System, etwa die Installation einer Anwendung oder eines Treibers, Probleme verursacht. Sie hilft Ihnen aber nicht dabei, Hardwareprobleme zu untersuchen.

D. **Falsch:** Die Systemabbild-Wiederherstellung stellt Ihre Systemkonfiguration aus einer Systemabbildsicherung wieder her, die Sie vorher angefertigt haben. Normalerweise wählen Sie diese Option, wenn Ihre Festplatte defekt war oder vollständig gelöscht werden musste. Die Systemabbild-Wiederherstellung hilft nicht dabei, Hardwareprobleme zu untersuchen.

5. **Richtige Antwort: C**

A. **Falsch:** *Bootmgr.exe* ist der Windows-Start-Manager. Er führt den Startprozess aus, aber Sie können damit keine Startoptionen bearbeiten.

B. **Falsch:** *Winload.exe* ist das Betriebssystemladeprogramm von Windows. Es lädt das ausgewählte Betriebssystem, aber Sie können damit keine Startoptionen bearbeiten.

C. **Richtig:** Mit *Bcdedit.exe* bearbeiten Sie Startoptionen. Sie können mit diesem Tool auch BCD im Remotezugriff verwalten und BCD ändern, wenn das System von einem anderen Medium gestartet wird als dem, auf dem der BCD-Speicher liegt.

D. **Falsch:** Windows 7 benutzt das Tool *Winresume.exe*, um aus dem Ruhezustand zu starten. Sie können damit keine Startoptionen bearbeiten.

Lektion 3

1. **Richtige Antwort: C**

   A. **Falsch:** Damit wird die Version der Datei wiederhergestellt, die am Abend vorher vorlag. Der Benutzer würde alle Änderungen verlieren, die er heute vorgenommen hat.

   B. **Falsch:** Vorgängerversionen umfassen Versionen aus der Datensicherung, die am Abend vorher durchgeführt wurde, sowie Schattenkopien. Die letzte Schattenkopie ist wahrscheinlich 2 Tage alt, weil bei der Installation des Grafikkartentreibers ein Wiederherstellungspunkt erstellt wurde. Unter den Vorgängerversionen befindet sich keine Version der Datei, die der Benutzer versehentlich gelöscht hat.

   C. **Richtig:** Der Benutzer hat die Datei erst vor Kurzem gelöscht, daher befindet sie sich noch in seinem Papierkorb. Sie enthält alle Daten, die darin enthalten waren, als sie gelöscht wurde.

   D. **Falsch:** Eine Systemwiederherstellung stellt keine gelöschte Benutzerdatei wieder her.

2. **Richtige Antworten: A und D**

   A. **Richtig:** Eine Systemabbildwiederherstellung stellt den Computer in dem Zustand wieder her, in dem er vor 3 Monaten war.

   B. **Falsch:** Alle Wiederherstellungspunkte sind verloren gegangen, als die Festplatte gelöscht wurde, daher hilft eine Systemwiederherstellung nichts. Der Benutzer muss die gesamte Software neu installieren, die er während der letzten 3 Monate installiert hat, die Updates der letzten 3 Monate einspielen (oder das von Windows Update erledigen lassen) und sicherstellen, dass seine Viren- und Spywaredefinitionen auf dem neusten Stand sind. Aber diese Möglichkeit wurde in der Aufgabe nicht beschrieben.

   C. **Falsch:** Alle Schattenkopien sind verloren gegangen, als die Festplatte gelöscht wurde. Außerdem ist die Bibliothek *Dokumente* nur ein virtueller Ordner.

   D. **Richtig:** Eine Systemabbildwiederherstellung stellt sicher, dass der Benutzer einen funktionierenden Computer hat. Der Inhalt seiner Bibliothek *Dokumente* ist allerdings 3 Monate alt. Er muss die Bibliothek *Dokumente* aus der Datensicherung wiederherstellen.

3. **Richtige Antworten: B und C**

   A. **Falsch:** Das Laufwerk *D:* enthält keine Systemdateien, daher brauchen Sie keine Systemeinstellungen zu speichern.

   B. **Richtig:** Damit werden immer, wenn ein Wiederherstellungspunkt erstellt wird, Vorgängerversionen der Dateien und Ordner auf dem Laufwerk *D:* angelegt.

C. **Richtig:** Damit werden 200 GByte der 500 GByte Festplattenkapazität für den Computerschutz reserviert.

D. **Falsch:** Damit werden nur 20 GByte der 500 GByte Festplattenkapazität für den Computerschutz reserviert. Sie wollen 200 GByte verwenden.

4. **Richtige Antwort: D**

   A. **Falsch:** Die Computerschutzeinstellungen sind nicht rückwirkend gültig. Alle Vorgängerversionen dieser Datei, die älter sind als 3 Monate, wurden bereits gelöscht. Wenn Sie nun den Festplattenplatz vergrößern, der für den Computerschutz reserviert ist, bringt das die gelöschten Dateien nicht zurück.

   B. **Falsch:** Bei der Systemwiederherstellung werden keine Benutzerdateien wiederhergestellt.

   C. **Falsch:** Die Computerschutzeinstellungen sind nicht rückwirkend gültig. Diese Option verhindert, dass Systemeinstellungen auf dem Volume gespeichert werden, wenn ein Wiederherstellungspunkt erstellt wird. Daher bleibt mehr Platz für Vorgängerversionen. Aber das bringt keine Datei zurück, die bereits gelöscht wurde, weil nicht genug Platz auf der Festplatte frei war.

   D. **Richtig:** Sie sollten die Konsole *Sichern und Wiederherstellen* benutzen, um die Datei wiederherzustellen. Das ist die einzige Möglichkeit, eine 6 Monate alte Datei wiederherzustellen.

5. **Richtige Antwort: C**

   A. **Falsch:** Eine Systemwiederherstellung stellt keinen beschädigten Favoritenordner wieder her.

   B. **Falsch:** Eine Systemabbildwiederherstellung stellt den Computer in dem Zustand wieder her, den er vor 3 Wochen hatte. Damit wird der Favoritenordner der Benutzerin wiederhergestellt, aber es fehlen alle Websites, die sie während der letzten 3 Wochen hinzugefügt hat. Auch alle anderen Dateien der Benutzerin sind 3 Wochen alt, sodass Sie sie aus einer Datensicherung oder aus Vorgängerversionen wiederherstellen müssten.

   C. **Richtig:** Damit stellen Sie den Favoritenordner der Benutzerin in dem Zustand wieder her, den er vor 24 Stunden hatte. Alle Websites, die seitdem hinzugefügt wurden, können von Hand erneut eingetragen werden.

   D. **Falsch:** Der Browserverlauf verrät, welche Sites die Benutzerin bisher besucht hat. Dies ist etwas anderes als der Inhalt des Favoritenordners.

Kapitel 14: Übung mit Fallbeispiel

Übung mit Fallbeispiel 1: Support für Datensicherung und Wiederherstellung

1. In dieser Situation sind Schattenkopien der Datei vorhanden. James sollte dem Benutzer raten, seine Datei wiederherzustellen, indem er mit der rechten Maustaste darauf klickt, den Befehl *Vorgängerversionen wiederherstellen* wählt und die neuste Schattenkopie auswählt.

2. Automatisch geplante Datei- und Ordnersicherungen speichern die Bibliothek *Dokumente* aller Benutzer, die Konten auf dem Computer haben. Der Sohn der Benutzerin kann seine Datei mit dem Assistenten *Dateien wiederherstellen* aus der Datensicherung wiederherstellen.
3. Die Systemwiederherstellung kann das Computersystem auf einen Wiederherstellungspunkt zurücksetzen, der erstellt wurde, bevor die neue Software installiert wurde. Dabei werden keine Benutzerdateien gelöscht oder geändert, die momentan auf dem Computer gespeichert sind. Es ist allerdings ratsam, wichtige Dateien zu sichern, bevor eine Systemwiederherstellung durchgeführt wird. (Das gilt genauso für alle anderen größeren Operationen.)
4. Die Kundin kann ein Systemabbild nicht auf den Datenträger legen, der das Betriebssystem enthält. Sie muss die Datensicherung auf eine externe Festplatte oder DVDs schreiben.

Übung mit Fallbeispiel 2: Beseitigen von System- und Konfigurationsproblemen

1. Don hat mehrere Möglichkeiten. Er kann beispielsweise in den erweiterten Startoptionen mit *Abgesicherter Modus* oder *Anzeige mit niedriger Auflösung aktivieren (640x480)* starten. Er kann auch eine Systemwiederherstellung durchführen. Am schnellsten bekommt er seinen Computer aber wieder zum Laufen, indem er die Option *Letzte als funktionierend bekannte Konfiguration (erweitert)* auswählt. Weil Don sich nicht angemeldet hat, seit der Treiber installiert wurde, startet der Computer daher mit dem vorher installierten Treiber.
2. Wenn Don eine Systemabbildwiederherstellung durchführt, bekommt er wieder einen funktionierenden Computer, aber er hat dann ein Systemabbild benutzt, das 3 Monate alt ist. In diesem Fall müsste Don die installierten Benutzerdateien und sein Benutzerprofil aus Datei- und Ordnersicherungen wiederherstellen und alle Anwendungen erneut installieren, die er während der letzten 3 Monate installiert hat. Eine Systemabbildwiederherstellung ist die letzte Rettung für den Fall, dass ein Festplattenlaufwerk vollständig gelöscht wurde.
3. Würden 90 Prozent der Festplattenkapazität für den Computerschutz reserviert, stünden nur 10 Prozent zum Speichern der aktuellen Benutzerdateien zur Verfügung. Das ist praktisch immer unsinnig. Die Einstellung 40 Prozent erlaubt es, Schattenkopien angemessen lang aufzubewahren, ohne dass die Hauptaufgabe der Festplatte beeinträchtigt wird.

Glossar

Anhebung der Rechte Eine Anhebung der Rechte ermöglicht die Durchführung von Arbeiten, die sich nicht mit den Rechten eines Standardbenutzers durchführen lassen.

AppLocker-Richtlinie Eine Richtlinienart, die sich in den Editionen Windows 7 Enterprise und Ultimate zur Beschränkung der Ausführung von Anwendungen auf der Basis von speziellen Identitätsinformationen verwenden lässt.

Ausgehende Regel Eine Firewallregel für den Datenverkehr eines Computers, der an einen externen Empfänger gerichtet ist.

Bereitstellen (deploy) Sie stellen ein Systemabbild bereit, indem sie es auf einem oder mehreren Zielcomputern installieren.

Bereitstellen im Dateisystem (mount) Sie stellen ein Systemabbild im Dateisystem bereit (oder »mounten« es), indem Sie es so ins Dateisystem einbinden, dass die im Abbild enthaltenen Informationen verfügbar sind und Sie Komponenten wie Treiber, Updates und Sprachpakete hinzufügen oder entfernen können.

Bereitstellungsfreigabe Ein freigegebener Netzwerkordner, der ein Systemabbild enthält, das bereitgestellt werden kann, sowie alle weiteren Dateien, die für die Bereitstellung erforderlich sind, beispielsweise Antwortdateien für die unbeaufsichtigte Installation.

Bevorzugtes Drahtlosnetzwerk Ein Drahtlosnetzwerk, zu dem ein Drahtlosclient eine Verbindung herzustellen und sich zu authentifizieren versucht. Gewöhnlich sind in der Liste der bevorzugten Netzwerke solche Netzwerke enthalten, zu denen der Client zuvor Verbindungen hergestellt hat.

Bibliothek Eine virtuelle Sammlung von Ordnern, meistens mit ähnlichen Inhalten.

BranchCache Eine Technologie, die es ermöglicht, Dateien, die auf Windows Server 2008 R2-Remoteservern gespeichert sind, im LAN einer Zweigstelle zwischenzuspeichern.

Datenwiederherstellungsagent (DRA) Ein Datenwiederherstellungsagent ist ein Benutzerkonto mit einem speziellen Zertifikat, das für den Zweck der Datenwiederherstellung verwendet wird.

Defragmentierung Eine Datei wird als fragmentiert bezeichnet, wenn sie auf dem Datenträger nicht in aufeinanderfolgenden Sektoren gespeichert ist. Bei einer Defragmentierung werden die Dateien so auf dem Datenträger angeordnet, dass sie wieder in aufeinanderfolgenden Sektoren gespeichert sind.

DirectAccess Eine Technologie, die es Windows 7-Clients ermöglicht, eine stets aktive IPv6-Verbindung zum internen Netzwerk einer Organisation herzustellen.

Dual-Boot Eine Konfiguration, die dem Benutzer beim Start des Computers die Auswahl des zu verwendenden Betriebssystems ermöglicht.

Dummywiederherstellung Mit einer Dummywiederherstellung ist eine Wiederherstellung gemeint, bei der Dateien und Ordner nicht am Originalspeicherort wiederhergestellt werden, sondern an einem anderen Ort. Mit einer Dummywiederherstellung können Sie den Wiederherstellungsvorgang und den ordnungsgemäßen Zustand der Dateien und Ordner überprüfen.

Eingehende Regel Eine Firewallregel für den Datenverkehr, der von einer externen Quelle an den Computer gerichtet ist.

Ereignisabonnement Ein Ereignisabonnement ist eine Konfiguration, die eine Übermittlung von Ereignisprotokolleinträgen von

einer Quelle zu einem Sammlungscomputer ermöglicht. Abonnements können von der Quelle oder vom Sammler eingerichtet werden.

Ereignisprotokoll Ein Ereignisprotokoll enthält Einträge über Ereignisse, die während des Betriebs des Computers aufgetreten sind, beispielsweise über den Start oder Stopp von Diensten oder Anwendungen. Manche Ereigniseinträge betreffen normale Vorgänge, andere enthalten Hinweise auf Fehler, zum Beispiel den erfolglosen Versuch, einen bestimmten Dienst zu starten. Auch Zugriffe auf Dateien und Ordner lassen sich zum Beispiel durch entsprechende Ereignisprotokolleinträge überwachen.

Ereignisweiterleitung Bei der Ereignisweiterleitung werden Ereignismeldungen, die bestimmte Kriterien erfüllen, an einen Verwaltungs- oder Sammlungscomputer weitergeleitet.

Globale Adresse Eine IPv6-Adresse, die ein Gerät aus dem Internet bezeichnet. Globale Adressen müssen im Internet eindeutig sein.

Hashregel Eine Regel, die einen digitalen Fingerabdruck verwendet, der aus den binären Eigenschaften einer Datei errechnet wurde.

Heimnetzgruppe Ermöglicht die Ressourcenfreigabe in Heimnetzwerken.

Herausgeberregel Eine Regel, die eine Datei oder eine Dateigruppe auf der Basis der digitalen Signatur des Herausgebers verwendet, der die Datei oder die Dateien signiert hat.

InPrivate-Browsen Ein spezieller Modus des Internet Explorers, bei dem der Browserverlauf, Cookies und zwischengespeicherte Daten nach dem Ende der Browsersitzung nicht mehr verfügbar sind.

InPrivate-Filterung Ein Filtermodus, der die Datenmenge beschränkt, die beim Browsen im Internet an andere Anbieter gesendet wird.

Installationsabbild Das Systemabbild (gewöhnlich eine WIM-Datei), das Sie auf Zielcomputern bereitstellen.

IP-Adresse (IPv4 oder IPv6) Eine eindeutige Adresse in einem Computernetzwerk, die von Geräten dazu verwendet wird, sich gegenseitig zu identifizieren und miteinander zu kommunizieren.

IP-Paket Die Grundeinheit, in der Daten ein IP-Netzwerk durchlaufen. Ein IP-Paket enthält neben den Nutzdaten eine Quell- und eine Zieladresse sowie einige Felder, die beispielsweise die Länge des Pakets angeben, eine Prüfsumme aufnehmen oder Flags mit Angaben darüber enthalten, ob das Paket fragmentieren kann oder fragmentiert wurde.

Kompatibilitätsfix Mehrere Kompatibilitätsfixes bilden einen Kompatibilitätsmodus. Eine ältere Bezeichnung für einen Kompatibilitätsfix ist »Shim«.

Kompatibilitätsmodus Eine Sammlung von Kompatibilitätsfixen, auch Shims genannt, die die Verwendung von Programmen, die für ältere Windows-Versionen entwickelt wurden, unter Windows 7 ermöglicht.

Leistungsindikator Ein Leistungsindikator liefert Daten über eine bestimmte Ressource, zum Beispiel die Auslastung des Prozessors oder die Menge des freien Arbeitsspeichers.

Mehrstufige Authentifizierung Zur Authentifizierung sind zwei oder mehr Komponenten erforderlich. Unter Windows 7 bedeutet dies gewöhnlich eine Authentifizierung mit einer Smartcard und einem Kennwort.

Netbook Ein Computer mit kleinem Formfaktor, auch *Netbookcomputer* genannt.

Öffentliche Adresse Eine IPv4-Adresse, die ein Gerät aus dem Internet oder das LAN im Internet identifiziert. Öffentliche Adressen müssen im Internet eindeutig sein.

Offlinedateien Ermöglichen auch dann die Verwendung von Dateien, die in einem entsprechend konfigurierten freigegebenen Ordner liegen, wenn der Computer nicht mit dem Netzwerk verbunden ist.

Pfadregel Eine Regel, die eine oder mehrere Anwendungen anhand ihres Speicherorts angibt.

RAID (Redundant Array of Independent Disks) Zwei oder mehr Festplattenlaufwerke werden auf logischer Ebene so miteinander kombiniert, dass sich Volumes über zwei oder mehr Festplattenlaufwerke erstrecken, um eine höhere Leistung, bessere Fehlertoleranz oder beides zu erreichen. Windows 7 unterstützt RAID-0, RAID-1 und RAID-5.

RemoteApp Eine Form der Präsentationsvirtualisierung, bei der das Fenster einer Anwendung, die auf einem Server ausgeführt wird, auf einem Client angezeigt wird.

Richtlinie für Softwareeinschränkung Eine Richtlinienart, die auf allen Windows-Versionen verwendet werden kann, um die Ausführung von Anwendungen auf Grundlage bestimmter Identitätsinformationen zu beschränken.

Sammlungssatz Ein Sammlungssatz ist eine Gruppe von Leistungsindikatoren, mit der Sie auch über einen längeren Zeitraum Leistungsdaten erfassen und aufzeichnen können, um zum Beispiel die Wirkung von Optimierungsversuchen zu überprüfen. Zu diesem Zweck bestimmen Sie vor der Optimierung die Anfangsleistung des Computers und speichern diese Referenzwerte (die »Baseline«) für spätere Vergleiche.

Schattenkopie Eine Schattenkopie ist eine ältere Version einer Datei oder eines Ordners, die zusammen mit einem Wiederherstellungspunkt erstellt wurde.

Sicherer Desktop Ein spezieller Desktop, der den Benutzer dazu zwingt, auf die Eingabeaufforderung der Benutzerkontensteuerung zu reagieren, bevor er wieder mit dem Computer arbeiten kann. Diese Sicherheitsmaßnahme soll verhindern, dass Benutzer von Malware dazu verleitet werden, einer Anhebung der Rechte zuzustimmen, obwohl sie es gar nicht wollen.

Side-by-Side-Migration Die Übertragung der Benutzerprofildaten von einem alten Computer auf einen anderen Computer, auf dem das neue Betriebssystem installiert ist.

Solution Accelerator Eine Sammlung von herunterladbaren Dateien, die als Ergänzung zu den Installationsdateien größerer Softwarepakete zusätzliche Anleitungen und Tools bietet, sofern dies für die entsprechende Software sinnvoll ist.

Speicher *Vertrauenswürdige Herausgeber* Ein geschützter Bereich auf dem Datenträger, der digitale Zertifikate enthält, wie sie zum Beispiel zur Überprüfung der Signatur von Gerätetreibern verwendet werden.

Standardgateway Die IP-Adresse, an die ein Host aus dem Subnetz ein Datenpaket (oder IP-Paket) sendet, wenn sich die IP-Zieladresse nicht im lokalen Subnetz befindet. Die Standardgatewayadresse bezeichnet gewöhnlich eine Schnittstelle auf einem Router, über den externe Verbindungen hergestellt werden können. Im Falle eines SOHO oder eines kleinen Testnetzwerks ist das Standardgateway gewöhnlich der WAP oder ICS-Computer.

Startabbild Ein Betriebssystemabbild, mit dem sich ein Zielcomputer starten lässt und das die Bereitstellung eines Installationsabbilds ermöglicht. Aufzeichnungs- und Suchabbilder sind spezielle Arten von Startabbildern.

Subnetz Ein identifizierbarer separater Abschnitt eines Organisationsnetzwerks. Gewöhnlich werden Computer aus einem geografischen Bereich, aus einem Gebäude oder aus demselben LAN in einem Subnetz zusammengefasst. Eine IPv4-Adresse setzt sich aus der Adresse des Subnetzes (Subnetzadresse) und aus der Adresse (Hostadresse) eines Geräts aus dem Subnetz zusammen.

Subnetzmaske Eine Zahl, die angibt, welche Bits aus einer IPv4-Adresse die Subnetzadresse und welche Bits die Hostadresse darstellen.

Systemabbild Eine Datenträgerabbilddatei, die ein Betriebssystem enthält.

Systemabbild Eine Kopie aller Dateien und Ordner aus dem Betriebssystemvolume (und gegebenenfalls anderer Volumes) eines Com-

puters. Mit einer Systemabbildsicherung können Sie einen Computer in genau der Konfiguration wiederherstellen, in der er sich zum Zeitpunkt der Sicherung befand.

Systemwiederherstellung Bei einer Systemwiederherstellung wird ein Computer in den Zustand zurückversetzt, in dem er sich zu dem Zeitpunkt befand, an dem ein bestimmter Wiederherstellungspunkt erstellt wurde. Systemwiederherstellungen ändern keine Benutzerdateien.

Transparente Zwischenspeicherung Der Vorgang, bei dem Dateien, die von Remotedateiservern abgerufen werden, automatisch auf dem Client lokal zwischengespeichert werden, um den Zugriff zu beschleunigen, wenn die Roundtrip-Latenz zum Remoteserver einen vorgegebenen Schwellenwert überschreitet.

Treiberspeicher Ein geschützter Bereich auf dem Datenträger, der die Treiber für PnP-Geräte enthält.

Übernehmen von Änderungen (commit) Sie übernehmen Änderungen an einem Abbild, wenn Sie die vorgenommenen Änderungen auf dem bereitgestellten Quellabbild speichern.

Verbindungssicherheitsregel Eine Regel, mit der Authentifizierungsanforderungen für eine Verbindung festgelegt werden.

Verschlüsselndes Dateisystem (EFS) Eine Technologie zur Verschlüsselung einzelner Dateien oder Ordner für bestimmte Benutzerkonten.

Virtuelle Festplatte (Virtual Hard Disk, VHD) Eine Datei mit der Namenerweiterung *.vhd*, die sich wie ein separates Festplattenlaufwerk verwenden lässt. In älteren Betriebssystemen waren VHDs, die Systemabbilder enthielten, auf die Verwendung in virtuellen Computern beschränkt, die zum Beispiel mit Hyper-V, Virtual Server und Virtual PC erstellt wurden. Unter Windows 7 können Sie VHDs auch für die Verwendung in physischen Computern erstellen.

Vorbereitung (Staging) Ein Administrator kann einen Gerätetreiber auf seine Verwendung vorbereiten, indem er ihn im Treiberspeicher speichert. Anschließend kann auch ein Standardbenutzer das Gerät installieren.

Wiederherstellungspunkt Ein Wiederherstellungspunkt enthält Informationen über Registrierungswerte und andere Systeminformationen. Windows 7 erstellt automatisch einen Wiederherstellungspunkt, bevor es größere Änderungen an der Konfiguration vornimmt. Sie können Wiederherstellungspunkte auch manuell erstellen und den Computer in den Zustand zurückversetzen, in dem er sich zu dem Zeitpunkt befand, an dem ein bestimmter Wiederherstellungspunkt erstellt wurde.

Windows Automated Installation Toolkit (Windows AIK) Eine Sammlung von Beschreibungen und Tools für die Bereitstellung von Windows-Betriebssystemabbildern auf physischen oder virtuellen Zielcomputern.

Windows-Remoteshell Ein Tool, das die Ausführung von Befehlszeilenprogrammen auf einem Remotecomputer ermöglicht.

Windows-Vorinstallationsumgebung (Windows Preinstallation Environment, Windows PE) Eine stark vereinfachte Version eines Betriebssystems (wie Windows 7), das zur Bereitstellung von vollständigen Betriebssystemen auf Computern verwendet wird.

Wipe-and-Load-Migration Ein Vorgang, bei dem Benutzerprofildaten vom alten Betriebssystem exportiert und nach der Entfernung des alten Betriebssystems und der Installation des neuen Betriebssystems auf demselben Computer importiert werden.

Stichwortverzeichnis

.bat-Dateien 278
.cmd-Dateien 278
.com-Dateien 271, 276
.js-Dateien 278
.ocx-Dateien 278
.ps1-Dateien 278
.swm-Dateien 94
.vbs-Dateien 271, 278
.xml-Migrationsdateien 40
.zip-Dateien 742
32- und 64-Bit-Plattformen, Abbilder, architekturunabhängige Tools 70
6to4 333, 335

A

Abbilder, System
  Informationen 116f.
  Konfigurieren
    DISM 74ff.
    Offline Virtual Machine Servicing Tool 95f.
    Referenzabbild erstellen 58–71
    Sysprep 76–83
    Überblick 53
    Übung, Erstellen von startfähigen VHDs 104–107
    Übung, WIM-Abbild erstellen 83ff.
    Verteilen 71–74
    VHDs, native 88–93
    Vorabbereitstellen von Clientcomputern 102ff.
    WDS, Online-VHD-Bereitstellung 96–104
    WDS-Abbilder 73f.
    WIM2VHD (Windows Image to Virtual Hard Disk) 93ff.
    Windows Automated Installation Kit (Windows AIK) 55ff.
    Windows Imaging (WIM) 70f.
    Windows Preinstallation Environment (WinPE) 57
  Übung mit Fallbeispiel, Systemabbilder erstellen 110
Abbildschritte 175
Abbildverwaltung für die Bereitstellung *Siehe* DISM
Abgesicherter Modus 752
Abonnements, Ereignisse 679f.
Abwärtskompatibilität 116
ACLs (Access Control Lists) 39
ACT (Application Compatibility Toolkit) 258–262
Active Directory-Benutzer und -Computer 102ff.
Active Directory-Domänendienste (AD DS) 383, 452, 559
Active Directory-Zertifikatdienste 452, 520, 533f., *siehe auch* Zertifikate
ActiveX 627
AD DS (Active Directory Domain Services) 383, 452, 559
AD DS-Server 102
Adaptereinstellungen ändern 313
Add-Ons verwalten 633
Ad-hoc-Netzwerke 347, 358, 370ff.
Administrationscomputer 58f.
Administratorbestätigungsmodus 481
Administratorbestätigungsmodus für das integrierte Administratorkonto 481
Administratorrechte
  Benutzerkontensteuerung (UAC)
    Einstellungen 478ff.
    Richtlinien 480–486
    Secpol und die Konsole Lokale Sicherheitsrichtlinie 486f.
    Übersicht 477f.
    Übung, konfigurieren 487ff.
  Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
  Windows Installer-Regeln 277
Administratorrechte und Privilegien
  Datensicherung 741
  Überprüfung 201
Adressen
  IPv4 konfigurieren
    Adressierung 298–305
    Problembehandlung 308–319
    Überblick 297f.
    Übung, Konfigurieren 319–323
    Verbindung mit Netzwerk herstellen 305–308
  IPv6 konfigurieren
    Aufbau von Adressen 326–331
    IPv4-Kompatibilität 332–335
    Konnektivität 336–340
    Übung, Konfigurieren von IPv6-Verbindungen 341ff.
    Vorteile von IPv6 331f.
Advanced Encryption Standard (AES) 356ff.
Aktionspaket 137
Aktive Hubs 197
Aktivierung durch lokales Netzwerk 400
Aktivierung zurücksetzen 80f.
Aktualisieren 205, *siehe auch* Upgrades
Alle Administratoren im Administratorbestätigungsmodus ausführen 484
Analysieren des Datenträgers 227
Anmeldedaten speichern 493
Anmeldeinformationen 495f., 504–507, 741
Anmeldeinformationsverwaltung 493ff.
Anmelden über Remotedesktopdienste zulassen 496
Anmeldungen
  Anmeldeinformationsverwaltung 493ff.
  Remotedesktop 400
Antispyware 663–666
Antivirus 663–666
Antwortdatei
  Einstellungen speichern 64
  Erstellen 59–63, 138
  Paketinstallation 129
  Referenzinstallation erstellen 65f.
  Sysprep 79f.
  Überwachungsmodus 82
  Unattend.xml 126, 135–138

Anwendung hinzufügen, Assistent 126
Anwendungen
  Ereignisprotokolle 677
  Leistung 721
  RemoteApp 539f.
  Systemwiederherstellung 752
Anwendungen verwalten *Siehe auch* AppLocker
  Application Compatibility Toolkit (ACT) 258–262
  Hinzufügen, MDT 162ff.
  Inventar 172
  Kompatibilität, konfigurieren 255–258
  Richtlinien für Softwareeinschränkung 269–275
  Richtlinien zur Anwendungskompatibilitätsdiagnose 262f.
  Übersicht 253
  Übung, Beschränken von Anwendungen 284–288
  Übung, Kompatibilität 264ff.
  Übungen mit Fallbeispiel 292f.
  Wartung 124ff.
  WIM-Abbilder 119
  Windows XP Mode 263f.
Anwendungsidentität (Dienst) 275
Anwendungsinstallationen erkennen und erhöhte Rechte anfordern 484
Anwendungssteuerungsrichtlinien *Siehe* AppLocker
Anycast 330
Anzeige 713f.
API (Application Programming Interface), Kompatibilität 259
APIPA (Automatic Private Internet Protocol Addressing) 297, 304
AppData 738
Application Compatibility Toolkit (ACT) 258–262
Application Programming Interface (API), Kompatibilität 259
AppLocker
  Anwendungssteuerungsrichtlinien, Überblick 275
  Konfigurieren von Ausnahmen 282
  Regeln 275–282
  Richtlinien für Softwareeinschränkung 269–275
  Überwachung 283f.
  Übung, Beschränken von Anwendungen 284–288
Arbeitsspeicher 5, 197
Architekturunabhängige Tools 70
Assistent für neue eingehende (oder ausgehende) Regeln 389f.
Assistent für neue Verbindungssicherheitsregel 391ff.
Assistent für vergessene Kennwörter 500
Assistent zum Erstellen von Ordnerfreigaben 428
Assistent zum Hinzufügen von Features, DirectAccess 522
Assistent zum Hinzufügen von Features, Windows Server 2008 466
Assistent zur automatischen Erstellung von Regeln 282
Assistenten
  Anwendung hinzufügen 126
  Assistent für neue eingehende (oder ausgehende) Regeln 389f.
  Assistent für neue Verbindungssicherheitsregel 391ff.
  Assistent für vergessene Kennwörter 500
  Assistent zum Erstellen von Ordnerfreigaben 428
  Betriebssystem importieren 151
  Dateien wiederherstellen 769
  Dateien wiederherstellen, Assistent 774
  Datenträgerinitialisierung 233
  Drahtlosnetzwerkinstallations-Assistent 352
  Drucker hinzufügen 367
Assistenten *(Fortsetzung)*
  Einfache Aufgabe erstellen 678
  Features hinzufügen, DirectAccess 522
  Features hinzufügen, Windows Server 2008 466
  Hardware-Assistent 202
  MOF Generator 703
  Netzwerkdrucker hinzufügen 367
  Neue Anwendung 163f.
  Neue Sammlung erstellen 657
  Neue Tasksequenz 174
  Neuer Treiber, Assistent 152f.
  Regelerstellungsassistent 280
  Regeln automatisch generieren 282
  Systemwiederherstellungs-Assistent 751f.
  Windows-Bereitstellung 165
  Windows-Bereitstellungsdienste (WDS)
    Assistent zur Abbildaufzeichnung 73, 169
  Zertifikatverwaltung 503
Aufgaben, Aufgabenplanung 744
Aufwecken aus Ruhezustand 723
Aufzeichnungsabbilder, WDS 73, 99, 168f.
Ausführbare Dateien
  AppLocker-Regeln 276
  Problembehandlung für Programmkompatibilität 255
  Richtlinien für Softwareeinschränkung 271
  Wechseldatenträger, Richtlinien 232
Ausgehender Datenverkehr 389f., 461
Auslagerungsdateien, Einstellungen 714
Ausnahmen 381, 385f.
Ausstehende Computer 97
Authentifizierung
  Anmeldeinformationsverwaltung 493ff.
  Beheben von Problemen 500ff.
  Benutzerkontensteuerung (UAC)
    Einstellungen 478ff.
    Richtlinien 480–486
    Secpol und die Konsole Lokale Sicherheitsrichtlinie 486f.
    Übersicht 477f.
    Übung, konfigurieren 487ff.
  Benutzerrechte 496f.
  BitLocker-Voraussetzungen 561
  DirectAccess 516, 520
  Ereignisweiterleitung 679
  Interne Drahtlosadapter 355–358
  Kontorichtlinien 499f.
  Netzwerksicherheitsschlüssel 353
  Portbasierte 356ff.
  Remoteverwaltung 407f.
  Runas 495f.
  Smartcards 498f.
  Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
  Übung, Verwalten von Anmeldeinformationen 504–507
  Virtuelle private Netzwerke (VPNs) 531–534
  Windows-Firewall mit erweiterter Sicherheit (WFAS) 391ff.
  Zertifikate, verwalten 502ff.
Authentifizierung auf Netzwerkebene 401
Automated.xml 136
Automatic Private Internet Protocol Addressing (APIPA) 297, 304

Automatische Datensicherungen 740–743
Autorisierung
  Anmeldeinformationsverwaltung 493ff.
  Beheben von Authentifizierungsproblemen 500ff.
  Benutzerrechte 496f.
  Kontorichtlinien 499f.
  Runas 495f.
  Smartcards 498f.
  Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
  Übung, Verwalten von Anmeldeinformationen 504–507
  Zertifikate, verwalten 502ff.
Autounattend.xml 70

B

Backup Set-Ordner 741
Bandbreite, USB-Hostcontroller 198
Basisdatenträger 239, 241, 247f.
Basispartitionen 233
BCD (Startkonfigurationsdaten) 759f.
BCDBoot 70, 170
BCDEdit 92f., 170, 759f.
Befehlszeilentools
  BCDEdit 92f., 170, 759f.
  BitLocker, Manage-bde.exe 567
  Cipher.exe 451, 502ff.
  Defrag 228f.
  Diskpart, VHDs erstellen und anfügen 90f.
  DISM 55ff., 74ff., 116–122, 124, 127, 135–138
  Energieverwaltung 588f.
  Icacls 444f.
  Ipconfig 298
  IPv6-Konnektivität 336–340
  net share 429f.
  Netsh 308, 349–354, 461–466
  Netstat 317ff.
  PEimg.exe (Windows PE) 116
  Ping 310–313
  RoboCopy.exe 447
  Runas 495f.
  Secedit.exe 486f.
  Sysprep 76–83
  Treiberüberprüfungs-Manager 210f.
  Unattend.xml-Antwortdateien 135–138
  USMT (User State Migration Tool) 39–42
  Wbadmin 743
  WDSUTIL 97
  Weitere Informationen 674
  WIM2VHD 93ff.
  WinRS (Windows Remote Shell) 407f.
Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln 485
Benutzer
  Gruppe Remotedesktopbenutzer 403
  Runas 495f.
Benutzer wechseln 401
Benutzerdefinierte Berichte 658
Benutzerkonten
  Datenwiederherstellungsagent 559
  Freigegebene Ordner 426–430
Benutzerkontensteuerung (UAC)
  Einstellungen 478ff.
  Remoteunterstützung 403
  Richtlinien 480–486
  Secpol und die Konsole Lokale Sicherheitsrichtlinie 486f.
  Übersicht 477f.
  Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
  Übung, konfigurieren 487ff.
Benutzernamen 493ff., 498f.
Benutzerprofile
  Migration, Windows AIK 55ff.
  Migrieren von Benutzerprofildaten 34, 37ff.
  Übung mit Fallbeispiel, Migrieren von Benutzerdaten 49f.
  Übung, Migrieren von Benutzerdaten 43ff.
  Wiederherstellen 773f.
  Windows-EasyTransfer 35–39
Benutzerrechte 496f., 530
Benutzerstatus, Schritte 175
Berechtigungen
  Dateien und Ordner 440–447
  Drucker 433
  Effektive Berechtigungen 445
  Freigegebene Ordner 426–430
  Freigegebene Ressourcen 452–457, 472
  Konfigurieren mit Icacls 444f.
  NTFS-Berechtigungen 269
  Skriptregeln 278
  Vererben 444
  Vollzugriff 428
  Wechseldatenträger, Richtlinien 232
Bereitstellen *Siehe auch* Bereitstellen von Systemabbildern; DISM
  Netzwerkfreigabe 68ff.
  Updates 160f., 611
  WDS, Online-VHD-Bereitstellung 96–104
  Windows 7, weitere Informationen 70
Bereitstellen von Systemabbildern
  Abbilder verteilen 71–74
  Anwendungen, Wartung 124ff.
  Betriebssystempakete, Wartung 126–129
  Internationale Einstellungen 130ff.
  Manuelle Installationen 177
  Microsoft Deployment Toolkit (MDT)
    Anwendungen hinzufügen 162ff.
    Betriebssystemabbild hinzufügen 151f.
    Distributionsfreigaben erstellen 150f.
    Gerätetreiber hinzufügen 152f.
    Language Packs 162
    LTI-Medien 165
    Offlinedateien aktualisieren 161f.
    Programmordner 146
    Tasksequenzen 153–160
    Überblick 144–149
    Updates hinzufügen 160f.
    Verwalten und Verteilen von Abbildern, Überblick 149f.
    Windows PE-Optionen, Konfigurieren 164
  Paketinstallation 129f.
  SCCM 2007 172–177
  Treiber, Wartung 122f.

Bereitstellen von Systemabbildern *(Fortsetzung)*
Übung
Herunterladen, Installieren und Konfigurieren von MDT 2010 177–183
Offlineabbild bereitstellen und Language Packs installieren 139ff.
Übungen mit Fallbeispiel 187f.
Unbeaufsichtigte Wartung, Befehlszeile 135–138
WDS 165–172
WIM-Befehle, DISM 116–122
Windows PE-Abbilder, Wartung 133ff.
Windows-Editionen verwalten 132f.
Berichte *Siehe* Ressourcen, Leistungsüberwachung und Berichterstellung
Betriebssystem importieren, Assistent 151
Betriebssystem, Standard- 17f.
Betriebssystemabbild hinzufügen 151f.
Betriebssysteme *Siehe auch* Systemabbilder konfigurieren
Fingerabdrücke 382
Windows Automated Installation Kit (Windows AIK) 55ff.
Betriebssystempakete, Wartung 126–129
Bevorzugte Drahtlosnetzwerke 354f.
Bibliotheken
Dynamic Link Libraries (DLLs) 271, 278, 673
Freigeben 430, 433–436
WMI-Skriptingbibliothek 700
Bildschirm 583
Bildschirmdarstellung 257
Binärnotation 299f.
Biometrische Authentifizierung 498
BIOS, Windows XP Mode 263
BitLocker
Aktivieren 561–564
BitLocker To Go 564, 566f.
Datenwiederherstellungsagenten (DRAs) 559ff.
Modi 556f.
Offline-Migrationen 42f.
TPM-Chip 558
Übersicht 555f.
Übung, BitLocker To Go 568–571
Verschlüsselndes Dateisystem (EFS) und 449
BITS (Intelligenter Hintergrundübertragungsdienst) 148
Blockierungsregeln 276
Bluetooth 353
Boot Configuration Data *Siehe* BCD (Startkonfigurationsdaten)
BranchCache
Konfigurieren von Clients 461–466
Modus Gehosteter Cache 460
Modus Verteilter Cache 460f.
Transparente Zwischenspeicherung 577
Übersicht 459f.
Übung, BranchCache-Konfiguration 468f.
Windows Server 2008 466f.
Broadcastadresse 300
Browsereinstellungen 720

C

Cabinetdateien (.cab) 126f.
Catalogs-Ordner 743
CD
Datensicherungen 740
Startfähige Windows PE 66f.
Wechseldatenträger, Richtlinien 232
CIDR-Notation 301
CIM-Klassen (Common Information Model) 699f.
CIMOM (Common Information Model Object Manager) 697f.
CIM-Repository (Common Information Model) 697, 699
Cipher.exe 451, 502ff.
Clientcomputer *Siehe auch* Systemabbilder konfigurieren
Abbilder verteilen 71–74
Betriebssystempakete, Wartung 126–129
Datensicherungen, VHDs 88
Erkennung 173
Installieren, wenige 65
IP-Einstellungen 312
IP-Konfigurationen 305
Netzwerkfreigabe, Bereitstellen 68ff.
Remoteverwaltung
Remotedesktop 400–403
Remoteunterstützung 403ff.
Übung, Remoteverwaltungsoptionen 408–413
Übungen mit Fallbeispiel 416
Windows-Remoteverwaltung 406ff.
Vorabbereitstellen 102ff.
Clientseitige Zielzuordnung aktivieren 612
Clientseitiges Rendering (CSR) 367
COA (Certificate of Authenticity) 81
Common Information Model Object Manager (CIMOM) 697f.
Common Information Model-Repository (CIM) 697, 699
Compatibility Administrator 259
Complete PC-Sicherung 745
Computer reparieren 751
Computerintegritätsprüfung 658–661
Computerschutz 776f.
Cone-NATs 335, *siehe auch* NAT (Network Address Translation)
Configuration Manager 2007 161, 173f., 176
Copype.cmd 66f.
Cscript 93
CSR (Clientseitiges Rendering) 367

D

Data Collector Set *Siehe* Sammlungssätze (DCS)
Data Execution Prevention *Siehe* Datenausführungsverhinderung (DEP)
Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren 485
Dateibasierter Speicher 70
Dateien
Benutzerprofile wiederherstellen 773f.
Beschädigte 120
Beschädigte oder gelöschte Dateien wiederherstellen 768–774
Datensicherung 740–743
Datenträgerbereinigung 225ff.
Freigeben *Siehe auch* Virtuelle private Netzwerke (VPN)
Bibliotheken 430
BranchCache, Konfigurieren von Clients 461–466
BranchCache, Modus Gehosteter Cache 460
BranchCache, Modus Verteilter Cache 460f.
BranchCache, Übersicht 459f.
BranchCache, Windows Server 2008 466f.

Dateien / Freigeben *(Fortsetzung)*
Datei- und Ordnerberechtigungen 440–447
DirectAccess 526
Drucker 431ff.
Freigegebene Ordner 425–430
Netzwerk- und Freigabecenter 421f.
Überwachung konfigurieren 447ff.
Übung, BranchCache-Konfiguration 468f.
Übung, Freigeben von Ressourcen 433–437
Übung, Verschlüsselung und Berechtigungen 452–457
Übungen mit Fallbeispiel 472
Verschlüsselndes Dateisystem (EFS) 449–452
Gerätetreiber 206
Migrieren von Benutzerprofildaten 34
Offlinedateien 574–582
Pfadregeln 272f., 280
Übung
Konfigurieren einer Datei- und Ordnersicherung 745ff.
Migrieren von Benutzerdaten 43ff.
Wiederherstellen umbenannter Dateien 778–781
Übung mit Fallbeispiel, Migrieren von Benutzerdaten 49f.
User State Migration Tool (USMT) 39–42
Verwalten 693
Volumeschattenkopiedienst (VSS) 773
Wiederherstellen von Vorgängerversionen 772
Windows-EasyTransfer 35–39
Dateien aus der Zwischenspeicherung ausschließen, Richtlinie 578
Dateien wiederherstellen, Assistent 769, 774
Dateihash, Definition 280
Dateinamenserweiterungen, Richtlinien für Softwareeinschränkung 271
Dateiprotokollierung (Profilerstellung) 134
Dateisignaturverifizierung (Sigverif) 215
Dateisystemfehler automatisch korrigieren 230
Dateiverschlüsselungszertifikate verwalten 502ff.
Datenausführungsverhinderung (DEP) 715
Datensammlungspakete 258
Datensicherung *Siehe auch* Sichern und Wiederherstellen-Konsole; Wiederherstellung, Daten
Anmeldeinformationsverwaltung 493ff.
Systemabbildsicherungen 743ff.
Thick-Abbilder (vollständige) 148
Übung, Konfigurieren einer Datei- und Ordnersicherung 745ff.
Übungen mit Fallbeispiel 785f.
Zeitplan 735–743
Datenträger *Siehe auch* Datenträgerverwaltungstool; Diskpart
Basis- und dynamische Datenträger 234ff.
Datensicherungsziel 737, 740
Diskette 232
Dynamische Datenträger 94, 238f., 241, 247f.
Externe Festplatten 227ff., 715f.
Feste Größe 94
MBR-Festplatten 239
Nutzung 776f.
Partitionen benutzen 233f.
Reaktivieren dynamischer Datenträger 238f.
Richtlinien 230ff.
Systemwiederherstellung 753
Übung mit Fallbeispiel, Verwalten 251
Datenträger *(Fortsetzung)*
Übung, Konfigurieren von Richtlinien und Konvertieren von Datenträgern 246ff.
Verschieben 237f.
Verwalten von Datenträgervolumes 239–245
Wartung 225–232
Datenträgerbereinigung 225ff.
Datenträgerinitialisierung, Assistent 233
Datenträgerschritte 175
Datenträgerverwaltungstool
Basis- und dynamische Datenträger, Konvertierung 235f.
Erstellen von Datenträgervolumes 239ff.
Größe von Volumes ändern 244f.
Löschen von Volumes 245
Partitionen benutzen 233f.
Reaktivieren dynamischer Datenträger 238f.
Stripesetvolumes erstellen 241
Übergreifende Volumes erstellen 240
VHDs anfügen und trennen 90
VHDs, native 88
Datenwiederherstellungsagenten (DRAs) 559ff.
Datum und Uhrzeit, Einstellungen 13
DCOM (Distributed Component Object Model) 708
DCS (Sammlungssätze) 651, 654–661, 730
Debuggen *Siehe auch* Problembehandlung
Betriebssystem auf VHD 94
Netzwerkstatistiken 317ff.
Startkonfigurationsdaten 759f.
Debugmodus 756ff.
Deferred Procedure Calls (DPC) 721
Defragmentieren von Datenträgern 227ff.
DEP (Data Execution Prevention) 715
Deployment Image Servicing and Management *Siehe* DISM
Deployment Workbench 72, 146–149, 162ff.
Designierte Dateitypen 271
Desktop
Datensicherung 738
Migrieren von Benutzerprofildaten 34
Remotedesktop 400–403, 408ff., 496f., 537–540
Sicherer Desktop 482, 485
DHCP (Dynamic Host Configuration Protocol) 165, 297, 302f., 305
Dialogfeld Dateifreigabe 426
Dialogfeld Erweiterte Freigabe 427
Dienste, Ereignisprotokolle 677
Dienste-Konsole 711ff.
Digitale Signaturen 484
Benutzerkontensteuerung (UAC) 486
Gerätetreiber 212–215
Überprüfung 201
Digitale Zertifikate *Siehe* Zertifikate
Digitaler Fingerabdruck 273, 280
Direct Access
Clientkonfiguration 517–521
Heimnetzgruppen 423
Problembehandlung 519ff.
Server konfigurieren 521–526
Übersicht 513, 515ff.
Übung, mit Netsh konfigurieren 526f.
Übungen mit Fallbeispiel 551
DirectAccess-Verwaltungskonsole 522

DirectX-Diagnose (DXdiag) 213ff.
Diskette 232
Diskpart
  Basis- und dynamische Datenträger, Konvertierung 235f.
  Erstellen von Volumes 239f., 242, 244
  Format, erstellte Volumes 70
  Größe von Volumes ändern 244f.
  Löschen von Volumes 245
  Netzwerkfreigabe, Bereitstellen 68ff.
  Partitionieren von Festplatten 234
  Reaktivieren dynamischer Datenträger 238f.
  Stripesetvolumes erstellen 242
  Übergreifende Volumes erstellen 240
  VHDs erstellen und anfügen 90f.
  VHDs, native 88
DISM
  Anwendungen, Wartung 124
  Beschreibung 57
  Betriebssystempakete, Wartung 127
  Systemabbilder konfigurieren und ändern 55ff.
  Überblick 74ff.
  Unbeaufsichtigte Wartung, Befehlszeile 135–138
  WIM-Befehle, Bereitstellen eines Abbilds 116–122
DISM (Deployment Image Servicing and Management, Tool zur Abbildverwaltung für die Bereitstellung)
  Systemabbilder konfigurieren und ändern 55ff.
Distributed Component Object Model (DCOM) 708
Distributed Management Task Force (DMTF) 699f.
Distributionsfreigabe 137, 144, 150f., 181ff.
DLLs (Dynamic Link Libraries) 271, 278, 673
DMTF (Distributed Management Task Force) 699f.
DNS *Siehe* Domain Name System (DNS)
Domain Name System (DNS)
  IPv4 konfigurieren 297
  Netzwerkdienste 302f.
  Server, IPv6-Adressen hinzufügen 338
  Server, Ping-Test 311
  Verwalten 693
  WDS 165
  Windows-Firewall mit erweiterter Sicherheit (WFAS) 390
Domänennetzwerke 383
Downloads, Multimedia 721
Downloads-Ordner 738
DRA (Data Recovery Agent) 559ff.
Drahtlosgeräte 346
Drahtlosnetzwerk, Eigenschaften 353, 362
Drahtlosnetzwerke verwalten 354
Drahtlosverbindungen
  Drahtlosnetzwerkinstallations-Assistent 352
  IPv4-Netzwerkverbindungen 307
  Netzwerke 346, 349–354, 359, 678
  Problembehandlung 361–365
  Sicherheit 355–358, 365
  Übung mit Fallbeispiel, Drahtlosnetzwerke 376f.
Drahtloszugriffspunkt *Siehe* WAP (Wireless Access Point)
Drucken, Windows 7-Verbesserungen 367ff.
Drucker 368f., 431ff., 693
Drucker hinzufügen, Assistent 367
Druckverwaltung, MMC-Snap-In 367
Dual-Boot-Installationen 14–18
Dummywiederherstellung 768
DVD
  Datensicherung 740
  Install.wim-Datei bereitstellen 119
  Installationsquelle vorbereiten 6
  Startfähige 57, 66f., 165
  Suchabbilder 167f.
  Übung, Erstellen von Windows PE-Start-DVD 83ff.
  Wechseldatenträger, Richtlinien 232
DXdiag (DirectX-Diagnose) 213ff.
Dynamic Host Configuration Protocol (DHCP) 165, 305, 390
Dynamic Link Libraries (DLLs) 271, 278, 673
Dynamische Datenträger 94, 238f., 241, 247f.
Dynamische Partitionen 233

E

EAP (Extensible Authentication Protocol) 357
Easy Connect 404
EasyTransfer-Kabel 36
Edgegeräte 391
Editionsfamilien, Abbilder 132
Editor für lokale Gruppenrichtlinien 204, 230ff., 447ff.
Effektive Berechtigungen 445
EFS (Encrypting File System) 449–452, 500, 502ff., 556
Eftsboot.com 67
Eigene Dateien wiederherstellen 769
Eigener Computer, Zonenregeln 274
Eigenschaften von Internet Protocol Version 4 (TCR/IPv4) 308
Eigenschaften von Internet Protocol Version 6 (TCP/IPv6) 338f.
Einfache Aufgabe erstellen, Assistent 678
Eingabe-/Ausgabe-Adressbereich, Ressourcen 197
Eingabeaufforderungen, Benutzerkontensteuerung 482f.
Eingabegebietsschema 131f.
Eingehender Datenverkehr 389f., 461
Eingeschränkte Sites 274
Einladungen, Remoteunterstützung 404
Einstellungen *Siehe auch* Einstellungen, Netzwerk
  Antwortdatei 59, 64
  Benutzerkontensteuerung (UAC) 478ff.
  Dateien kopieren und wiederherstellen 734
  Datum und Uhrzeit 13
  Energiesparpläne 582–585, 587ff.
  Erweiterte Freigabeeinstellungen 422, 431
  Geräte 196
  Internationale 130ff.
  Internet Explorer, Sicherheit 624–627
  Leistung
    CIM-Klassen 699f.
    CIM-Repository 699
    Leistungsoptionen 713ff.
    WMI, CIMOM 698
    WMI, Überblick 693–697
    WMI-Anbieter 698
    WMI-Skriptingbibliothek 700
    WMI-Verbraucher 700
    WMI-Verwaltung 700–709
  Migrieren von Benutzerprofildaten 34, 37ff.
  Offlineeinstellungen 428
  Systemwiederherstellung 751–755
  Wartungscenter 664
  Windows PE-Abbilder 134
  Windows-Firewall 386

Einstellungen, Netzwerk *Siehe auch* Einstellungen
Ad-hoc-Netzwerke 358
Drahtloscomputer hinzufügen 349–354
Drahtlosnetzwerke
Problembehandlung 361–365
Sicherheit 365
Technologien 359
Verwalten 354f.
Drucken, Verbesserungen 367ff.
Interne Drahtlosadapter, Sicherheit 355–358
IPv4
Adressierung 298–305
Problembehandlung für Konnektivität 308–319
Überblick 297f.
Übung, Konfigurieren 319–323
Verbindung mit Netzwerk herstellen 305–308
IPv6
IPv4-Kompatibilität 332–335
Konfigurieren von Adressen 326–331
Konnektivität 336–340
Übung, Konfigurieren von IPv6-Verbindungen 341ff.
Vorteile von IPv6 331f.
Konnektivität
Überblick 345ff.
Verbindungen einrichten 347ff.
Verbindungen verwalten 360f.
Übung mit Fallbeispiel
Drahtlosnetzwerke 376f.
IPv4-Verbindungen 376
IPv6-Verbindungen 376
Übung, Erstellen von Ad-hoc-Netzwerken 370ff.
Einwählverbindungen 540–544
Einzelinstanzspeicher 71
El Torito-Startsektordatei 67
E-Mail-Daten 34–39
Encrypting File System *Siehe* Verschlüsselndes Dateisystem (EFS)
Energiebedarf 582–585, 587ff.
Energiesparmodus 400, 584
Energiesparpläne 582–585, 587–592
Energieverwaltung 196
Entwurfsspeicher 135
Ereignisabonnements 679f.
Ereignisanzeige 717f.
Ereignisse
AppLocker-Überwachungsprotokoll 283
Leistungsüberwachung und Berichterstellung 651–661
Problembehandlung für Leistung 717f.
Protokollierung und Weiterleitung 676–684, 693, 730
Überwachen 447ff.
WMI-Ereignisanzeige 707ff.
WMI-Ereignisregistrierung 706f.
Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind 486
Erkennungsmethoden 173
Erstellen
Abbilder 74
Antwortdateien, Windows SIM 80, 138
Aufzeichnungsabbild 99, 168f.
Datenträgervolumes 239
Distributionsfreigabe 137, 150f.
Erstellen *(Fortsetzung)*
Einfache Volumes 239
Energiesparplan, benutzerdefiniert 587
Ereignisabonnements 682ff.
Gespiegelte Volume (RAID-1) 242
Referenzabbild 58–71
Sammlungen, in Eingabeaufforderung 658
Sammlungssätze 656f.
Skripts für Netzwerkfreigabebereitstellung 69
Startfähige DVD 57
Startfähige Windows PE-Medien 66f.
Stripesetvolume mit Parity (RAID-5) 242ff.
Stripesetvolumes (RAID-0) 241f.
Suchabbilder, WDS 167f.
Übung
Energiesparplan, benutzerdefiniert 589–592
Erstellen von Ad-hoc-Netzwerken 370ff.
Startfähige VHD 104–107
WIM-Abbild 83ff.
VHD, native 89ff.
WDS, Suchabbild 100
WFAS-Regeln 389f.
Erweiterte Freigabeeinstellungen 309, 348, 422, 431
Erweiterte Startoptionen 756ff.
Erweiterte Wiederherstellungsmethoden 754
Erzwingen der Treibersignatur deaktivieren 213
Erzwingen von Regeln 271
Ethernet 317ff., 346–349
Event Tracing for Windows *Siehe* ETW (Ereignisablaufverfolgung für Windows)
Exclusive OR (XOR) 333
Exportieren
Firewallkonfiguration 393
Sicherheitsrichtlinien 486f.
Startabbild, WDS 101
Extensible Authentication Protocol (EAP) 357
Extensible Firmware Interface (EFI) 103
Extensible Markup Language *Siehe* XML-Dateien (Extensible Markup Language)
Externe Festplatten 227ff., 715f.

F

Failoverschutz 126–129, 242ff.
Farben 367
FAT-Dateisystem 7, 440, 447, 450, 738, 777
Favorites-Ordner 738
Featureeigenschaften 137
Feature-IDs 137
Fehler, Festplatte 230
Fehler, überwachen 661f.
Fehlerbehebung *Siehe* Problembehandlung
Fehlertoleranz 241
Feste Größe, Datenträger 94
Festplatten 740, 753, *siehe auch* Datenträger
Fingerabdrücke von Betriebssystemen 382
Firewalls
BranchCache, Konfigurieren von Clients 461f., 464f.
DirectAccess 516, 526
Ereignisweiterleitung 679
Netzwerkeinstellungen konfigurieren 315ff.
Ping-Tool 310–313

Firewalls *(Fortsetzung)*
Wartungscenter 663–666
Windows Update-Clients 608
Windows-Firewall 381–387
Windows-Firewall mit erweiterter Sicherheit (WFAS) 387–394
Format Prefix (FP) 328
FQDNs *Siehe* Vollqualifizierte Domänennamen (FQDNs)
Freigabeberechtigungen 430
Freigabeeinstellungen, erweiterte 348
Freigeben von Ressourcen *Siehe auch* Virtuelle private Netzwerke (VPN)
Bibliotheken 430
BranchCache, Konfigurieren von Clients 461–466
BranchCache, Modus Gehosteter Cache 460
BranchCache, Modus Verteilter Cache 460f.
BranchCache, Übersicht 459f.
BranchCache, Windows Server 2008 466f.
Datei- und Ordnerberechtigungen 440–447
DirectAccess 526
Drucker 431ff.
EFS und Heimnetzgruppen 452
EFS-Wiederherstellung 451f.
Netzwerk- und Freigabecenter 421f.
Ordner 425–430, 581, 693
Überwachung, konfigurieren 447ff.
Übung
BranchCache-Konfiguration 468f.
Freigeben von Ressourcen 433–437
Verschlüsselung und Berechtigungen 452–457
Übungen mit Fallbeispiel 472
Verschlüsselndes Dateisystem (EFS) 449–452
Fully Qualified Domain Name *Siehe* Vollqualifizierte Domänennamen (FQDNs)

G

Gemeinsame Nutzung der Internetverbindung *Siehe* ICS (Internet Connection Sharing)
generalize, Konfigurationsdurchlauf 79
Geplante Tasks 693
Geräte und Treiber
Application Compatibility Manager 258
Benutzen mit Gerätetreiber 204ff.
Dateisignaturverifizierung 215
Drahtlos, Verbindungen zu WAP 346
Drucker freigeben 431
Installation, Überblick 199
Installieren, Windows Update 200f.
Konfigurieren von Installationsrichtlinien 203f.
Konfliktlösung 207–210
Nicht-PnP-Geräte installieren 202
Out-of-Box 66
Plug & Play, beibehalten 80
Staging 200f.
Treibersignierung und digitale Signaturen 212–215
Treiberüberprüfungs-Manager 210f.
Übung mit Fallbeispiel, Signierungsrichtlinie 251
Übung, Konfigurieren von Richtlinien und Treibersuche 216–222
Updates 205
Geräteinstallationseinstellungen 200
Geräte-Manager 193–199, 205
Geschützter Modus, Internet Explorer 625
Gespiegelte Volumes 235, 237, 242
GlobalCatalog.wbcat 743
Globale Unicastadressen 328
Globally Unique Identifier (GUID) 124
GPT-Festplattenpartitionen 233, 239
Größe von Volumes ändern 244f.
Gruppe Ereignisprotokollleser 680
Gruppe Jeder 426–430
Gruppe Remotedesktopbenutzer 403, 496f.
Gruppenrichtlinien *Siehe auch* Richtlinien
Administrator-Konto 496
Benutzerkontensteuerung (UAC) 480–486
Benutzerrechte 496f.
BitLocker-Voraussetzungen 561
BranchCache 461–466
DirectAccess 517–526
Energieeinstellungen 587
Ereignisabonnements 681f.
Gerätetreiber 200f., 212
Internet Explorer, Kompatibilitätsansicht 624
Kontorichtlinien 499f.
Remotedesktopgateway 539
Remoteverwaltung 407f.
Standortabhängiges Drucken 368f.
Windows Update 613ff.
Gruppenrichtlinienobjekte 521–526
GUID (Globally Unique Identifier) 124

H

HAL (Hardware Abstraction Layer) 92
Handles 673
Handymodems 358
Handys 230ff.
Hardware *Siehe auch* Geräte und Treiber; Datenträger
Application Compatibility Manager 258
BitLocker Voraussetzungen 561
Energiesparpläne 582–585, 587ff.
Hardware Abstraction Layer (HAL) 92
Inventar 172
Leistungsüberwachung und Berichterstellung
CIM-Klassen 699f.
CIM-Repository 699
Ereignisprotokollierung und -weiterleitung 676–684
Leistungsoptionen 713ff.
Netzwerkauslastung konfigurieren 719ff.
Problembehandlung 717f.
Process Explorer 673ff.
Ressourcenmonitor 669–673
Schreibcache konfigurieren 715f.
Task-Manager 718f.
Überblick 651–661
Übung, Leistungsüberwachung 684–690
Übung, Windows-Leistungsanalysetools 723ff.
Übungen mit Fallbeispiel 730f.
Wartungscenter 663–666
Windows Performance Toolkit (WPT) 721ff.
WMI, CIMOM 698
WMI, Überblick 693–697
WMI-Anbieter 698

Hardware / Leistungsüberwachung und Berichterstellung *(Fortsetzung)*
WMI-Dienst 699
WMI-Skriptingbibliothek 700
WMI-Verbraucher 700
WMI-Verwaltung 700–709
Zuverlässigkeit, Stabilität und Leistung 661ff.
RAM-Voraussetzungen, Windows XP Mode 263
Übung, Konfigurieren von Zugriffsrichtlinien und Konvertieren von Datenträgern 246ff.
Voraussetzungen für Windows 7 5
Windows 7 Upgrade Advisor 27
Hardware Abstraction Layer (HAL) 92
Hardware-Assistent 202
Hardwareressourcen, Msinfo32 209
Hashregeln 254, 270, 273, 278, 280
Heim- oder Arbeitsplatznetzwerke (privat) 383, 421f.
Heimnetzgruppe 431–436, 452
erstellen 21
Heimnetzgruppenverbindungen 423ff.
Help-Desk, Remotezugriff 403ff.
Herausgeberregeln 278ff.
Herunterfahren 401, 584, 723
Hexadezimalnotation 299f.
Hintergrunddienste 714
Hinzufügen von Treibern 122
Höchstleistung, Energiesparplan 582–585, 587ff.
Hotfixpatches 94
HTTP (Hypertext Transfer Protocol) 174, 679
HTTPS (Hypertext Transfer Protocol Secure) 174, 679
Hybridabbilder 149
Hybridnetzwerk 346
Hypertext Transfer Protocol (HTTP) 174, 679
Hypertext Transfer Protocol Secure (HTTPS) 174, 679
Hyper-V 88f.

I

IANA (Internet Assigned Numbers Authority) 304f.
Icacls 444f.
ICMP (Internet Control Message Protocol) 310–313
ICMPv4-Echoanforderungen 315
ICMPv6-Echoanforderungen 315, 339
ICMPv6-Netzwerkverkehr 526
ICS (Internet Connection Sharing) 302f., 305, 322f.
ID-Attribute 137
IEEE 802.11i-Standard 356ff.
IKEv2-Protokoll 530, 535
ImageX
Abbilder, Bereitstellen 116, 118
Abbilder, Informationen 117
Beschreibung 57
Netzwerkfreigabe, Abbild speichern 67f.
Systemabbilder aufzeichnen 55ff.
Systemstart von VHD 91
Wimscript.ini 67
Windows PE-Abbilder 133
Importieren, Firewallkonfiguration 393
In dynamischen Datenträger konvertieren 235
Informationsereignisse 679
Inhaltsabruf, Firewallregel 461
InPrivate-Modus 628–631
Install.wim 119, 166
Installation steht aus, Status 129
Installieren
Aufgaben nach der Installation 137
DVDs 119
Gerätetreiber 193, 203f., 206
Offline Virtual Machine Servicing Tool 95f.
Pakete, Faktoren 129f.
Referenzcomputer 65f.
Setup Analysis Tool 261
Sysprep 76–83
Übung
Durchführen einer Neuinstallation 18–21
Herunterladen, Installieren und Konfigurieren von MDT 2010 177–183
Windows AIK 83ff.
Übung mit Fallbeispiel, Windows 7-Installation 49
Updatedateien, manuell 608f.
Vorbereiten der Installationsquelle 6–9
WDS 165f.
Windows 7 9–18
Windows Automated Installation Kit (Windows AIK) 55ff.
Windows-EasyTransfer 36
Installieren von Abbildern, WDS 73, 98, 100f., 166f.
Intelligenter Hintergrundübertragungsdienst 148
Internationale Einstellungen 119, 121, 130ff.
Internationale Einstellungen, Konfigurationstool (Intlcfg.exe) 116
Interne Festplatten 227ff.
Interne Netzwerkressourcen 526
Internet *Siehe auch* Adressen; Internet Explorer
Private IPv4-Adressen 304f.
Remotedesktopverbindungen 401
Temporäre Dateien, Datenträgerbereinigung 225ff.
Verbindung gemeinsam nutzen 305
Internet Assigned Numbers Authority (IANA) 304f.
Internet Connection Sharing *Siehe* ICS (Internet Connection Sharing)
Internet Control Message Protocol (ICMP) 310–313
Internet Explorer *Siehe auch* Internet
Add-Ons und Suchanbieter 631ff.
Compatibility Test Tool 260
InPrivate-Modus 628–631
Kompatibilitätsansicht 623f.
Popupblocker 633f.
Sicherheitseinstellungen 624–627
SmartScreen-Filter 628
SSL-Zertifikate konfigurieren 634–637
Übung mit Fallbeispiel 646f.
Übung, InPrivate-Modus und Add-Ons 637–641
Zertifikatfehler 636
Zonenregeln 274
Internet Protocol Security (IPSec)
DirectAccess 515f.
Verbindungsregeln und -richtlinien 340, 393
Internet Protocol-Hypertext Protocol Secure (IP-HTTPS) 516
Internetoptionen, Konfigurieren 719ff.
Internetzonenregeln 274
Internetzwerk 313
Interrupt Request (IRQ) 197, 721
Interruptwellen 721

Intlcfg 74
Intranets 274, 329f.
Intra-Site Automatic Tunneling Addressing Protocol (ISATAP) 335
Ioctl_disk_performance-Datei 684
IP6-zu-IP4 516, 519
IP-Adressen 390
Ipconfig 298, 311, 336ff.
IP-HTTPS 516, 521
IP-Konfiguration, Problembehandlung 310–313
IP-Routing, Statistiken 317ff.
IPSec (Internet Protocol Security)
  DirectAccess 515f.
  Verbindungsregeln und -richtlinien 340, 393
IP-Sicherheitsrichtlinienverwaltung, Konsole 340
IPv4
  Adressierung 298–305
  DirectAccess 515f., 519
  Konfigurieren
    Problembehandlung für Konnektivität 308–319
    Überblick 297f.
    Übung, Konfigurieren von Netzwerkverbindungen 319–323
    Verbindung mit Netzwerk herstellen 305–308
  Netzwerkstatistiken 317ff.
  Remotedesktopverbindungen 401
  Übung mit Fallbeispiel, IPv4-Verbindungen 376
  Windows-Firewall mit erweiterter Sicherheit (WFAS) 390
IPv6
  Aufbau von Adressen 326–331
  IPv4-Kompatibilität 332–335
  Konnektivität 336–340
  Netzwerkstatistiken 317ff.
  Remotedesktopverbindungen 401
  Übung mit Fallbeispiel, IPv6-Verbindungen 376
  Übung, Konfigurieren von IPv6-Verbindungen 341ff.
  Vorteile 331f.
  Windows-Firewall mit erweiterter Sicherheit (WFAS) 390
ipv6.arpa 332
IPv6-Reverse-Lookupzone 332
ISATAP (Intra-Site Automatic Tunneling Addressing Protocol) 335

K

Kabelnetzwerk 346
Kennwörter
  Anmeldeinformationsverwaltung 493ff.
  Beheben von Authentifizierungsproblemen 500ff.
  Kontorichtlinien 499f.
  Remoteunterstützung 405
  Remotezugriff 408
  Runas 495f.
  Smartcards 498f.
  Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
  Übung, Verwalten von Anmeldeinformationen 504–507
  VPN-Authentifizierungsprotokolle 533f.
  Wiederherstellungskennwörter 559f.
Kennwortrücksetzdiskette 500
Kerberos V5-Protokoll 391
Kernelmodustreiber 261
Kernelspeicher 667
Kernnetzwerk, ausgehende Regeln 316
Kernnetzwerk, eingehende Regeln 316
Key Management Service (KMS) *Siehe* Schlüsselverwaltungsdienst (KMS)
Klassenansicht 702
Klassenexplorer 702
Klassenspeicher 699
KMS *Siehe* Schlüsselverwaltungsdienst (KMS)
KnowledgeBase-Kennungen 604f.
Kompatibilität, Anwendungen
  Abwärtskompatibilität 116
  Application Compatibility Toolkit (ACT) 258–262
  Konfigurieren von 255–258
  Richtlinien zur Anwendungskompatibilitätsdiagnose 262f.
  Übung, Windows 7-Kompatibilität 264ff.
  Übungen mit Fallbeispiel 292f.
  Windows XP Mode 263f.
Kompatibilitätsfix, Definition 259
Kompatibilitätsmodi, Definition 259
Komprimierte Dateien (.zip) 742
Komprimierte Ordner 450
Komprimierung, Datensicherung 734
Konfigurationsdurchläufe, Windows-Setup 78
Konfigurieren *Siehe auch* Konfigurieren von Systemabbildern
  Anwendungskompatibilität 255–258
  Berechtigungen, Icacls 444f.
  BranchCache, Konfigurieren von Clients 461–466
  BrancheCache-Server 460
  Computerschutz 762–766
  Computerschutz und Datenträgernutzung 776f.
  DirectAccess, Clientkonfiguration 517–521
  Ereignisabonnements 680ff.
  Firewallausnahmen 385f.
  Freigegebene Ordner 581
  Geräteinstallationsrichtlinien 203f.
  Heimnetzgruppeneinstellungen 433–436
  Internationale Einstellungen 130ff.
  Internet Explorer
    Add-Ons und Suchanbieter 631ff.
    InPrivate-Modus 628–631
    Kompatibilitätsansicht 623f.
    Popupblocker 633f.
    Sicherheitseinstellungen 624–627
    SmartScreen-Filter 628
    SSL-Zertifikate konfigurieren 634–637
    Übung mit Fallbeispiel 646f.
    Übung, InPrivate-Modus und Add-Ons 637–641
  IPv4
    Adressierung 298–305
    Problembehandlung für Konnektivität 308–319
    Überblick 297f.
    Übung, Konfigurieren von Netzwerkverbindungen 319–323
    Verbindung mit Netzwerk herstellen 305–308
  IPv6
    Aufbau von Adressen 326–331
    IPv4-Kompatibilität 332–335
    Konnektivität 336–340
    Übung, Konfigurieren von IPv6-Verbindungen 341ff.
    Vorteile von IPv6 331f.

Konfigurieren *(Fortsetzung)*
Leistungseinstellungen
CIM-Klassen 699f.
CIM-Repository 699
Leistungsoptionen 713ff.
WMI, CIMOM 698
WMI, Überblick 693–697
WMI-Anbieter 698
WMI-Dienst 699
WMI-Skriptingbibliothek 700
WMI-Verbraucher 700
WMI-Verwaltung 700–709
LTI-Medien 165
Netzwerkleistung 719ff.
Prozesse, Task-Manager 718f.
Remotedesktop 401ff.
Schreibcache 715f.
SSL-Zertifikate 634–637
Übung
Benutzerkontensteuerung (UAC) 487ff.
BitLocker To Go 568–571
BranchCache 468f.
Herunterladen, Installieren und Konfigurieren von MDT 2010 177–183
Remoteverbindungen 545ff.
Windows Update 618ff.
Windows-Firewall 394–397
WDS 165f.
Windows PE-Optionen 164
Windows Update 601–609
Konfigurieren des Standardbetriebssystems, Dual-Boot 17f.
Konfigurieren von Systemabbildern
DISM 74ff.
Offline Virtual Machine Servicing Tool 95f.
Referenzabbild erstellen 58–71
Sysprep 76–83
Überblick 53
Übung mit Fallbeispiel, Systemabbilder erstellen 110
Übung, Erstellen von startfähigen VHDs 104–107
Übung, WIM-Abbild erstellen 83ff.
Verteilen 71–74
VHDs, native 88–93
Vorabbereitstellen von Clientcomputern 102ff.
WDS, Online-VHD-Bereitstellung 96–104
WDS-Abbilder 73f.
WIM2VHD (Windows Image to Virtual Hard Disk) 93ff.
Windows Automated Installation Kit (Windows AIK) 55ff.
Windows Preinstallation Environment (WinPE) 57
Konflikte
Gerätetreiber 205, 207–210
Offlinedateien 574, 579ff.
Konnektivität
Ad-hoc-Netzwerke 358
Computer zu Computer 309
Drahtlosnetzwerke
Problembehandlung 361–365
Sicherheit 365
Technologien 359
Verwalten 354f.
Interne Drahtlosadapter, Sicherheit 355–358
IPv6 konfigurieren 336–340
Konnektivität *(Fortsetzung)*
Netzwerke
Drahtloscomputer hinzufügen 349–354
Überblick 345ff.
Verbindungen einrichten 347ff.
Verbindungen verwalten 360f.
Übung
Erstellen von Ad-hoc-Netzwerken 370ff.
Konfigurieren von IPv6-Verbindungen 341ff.
Übung mit Fallbeispiel
Drahtlosnetzwerke 376f.
IPv4-Verbindungen 376
IPv6-Verbindungen 376
Kontakte 738
Konto ist gesperrt 502
Kontosperrungsrichtlinien 499f., 502
Kopieren von Dateien 446f.

L

L2TP/IPsec 515, 530, 535
Language Packs 119, 121, 130–133, 139ff., 162, 187
Laptops *Siehe auch* Drahtlosverbindungen
Einwählverbindungen 540f.
Energiesparpläne 582–585, 587ff.
Freigegebene Ordner, konfigurieren 581
Offlinedateien 574–582
Synchronisierungscenter 579ff.
Transparente Zwischenspeicherung 577f.
Übung mit Fallbeispiel, Offlinedateien 596f.
Verloren gegangene 555
Laufwerkbuchstaben 237
Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPsec) 515
LDM (Logical Disk Manager) 234
Legacyhardware 202
Leistung
Defragmentieren von Datenträgern 227ff.
Dienste-Konsole 711ff.
Ereignisprotokollierung und -weiterleitung 676–684
Netzwerke, Konfigurieren 719ff.
Netzwerkstatistiken 317ff.
Problembehandlung 717f.
Process Explorer 673ff.
Ressourcenmonitor 669–673
Schreibcache konfigurieren 715f.
Stripesetvolumes mit Parity (RAID-5) 242ff.
Systemstart von VHD 91
Task-Manager 718f.
Übergreifende Volumes 240
Überwachung und Berichterstellung 651–661
Übung, Leistungsüberwachung 684–690
Übung, Windows-Leistungsanalysetools 723ff.
Übungen mit Fallbeispiel 730f.
Wartungscenter 663–666
Windows Performance Toolkit (WPT) 721ff.
WMI
Anbieter 698
CIM-Klassen 699f.
CIMOM 698
CIM-Repository 699
Überblick 693–697

Leistung / WMI *(Fortsetzung)*
WMI-Dienst 699
WMI-Skriptingbibliothek 700
WMI-Verbraucher 700
WMI-Verwaltung 700–709
Zuverlässigkeit, Stabilität und Leistung 661ff.
Leistungsüberwachung 652ff., 684–690
Lese-/Schreibzugriff auf Abbild 119
Lesen
Berechtigungen 440f.
Freigegebene Ordner 426–430
Leistung 243
Wechseldatenträger, Richtlinien 232
Lesen/Schreiben-Berechtigungen 426–430
Letzte als funktionierend bekannte Konfiguration 758, 761f.
Links-Ordner 738
Listenelemente 137
Lite Touch Installation (LTI) 72, 145, 165
Lizenz, Product Key 80f.
LoadState 41
Logical Disk Manager (LDM) 234
Logman 658
Lokale Sicherheitsrichtlinie 486f.
Lokale Standardbenutzergruppen 497
Lokales Intranet, Sicherheitseinstellungen 624
Lokales Subnetz 390
Loopbackadresse 330
Löschen von Dateien und Ordnern 440f.
Löschen von Volumes 245
LTI (Lite Touch Installation) 72, 145, 165

M

MAC (Media Access Control) 303, 332
Machine OOBE 63
MAK (Multiple Activation Key) 81
Malware *Siehe* Benutzerkontensteuerung (UAC)
Manage-bde.exe 567
Managed Object Format (.mof) 176
Massenspeicher
Migrationsspeichertypen 42
Voraussetzungen 5
MBR-Festplatten 239
MBSA (Microsoft Baseline Security Analyzer) 617f.
MDT (Microsoft Deployment Toolkit)
Anwendungen hinzufügen 162ff.
Betriebssystemabbild hinzufügen 151f.
Distributionsfreigabe erstellen 150f.
Language Packs 162
LTI-Medien 165
MDT 2010, Überblick 72f.
Offlinedateien aktualisieren 161f.
SCCM, Integration 176f.
Tasksequenzen 153–160
Überblick 144–149
Übung, Herunterladen, Installieren und Konfigurieren von MDT 2010 177–183
Updates hinzufügen 160f.
Verwalten und Verteilen von Abbildern, Überblick 149f.
Windows PE-Optionen, Konfigurieren 164
Media Access Control (MAC) 303, 332
MeinSpeicher 41
Meldungen 609f.
Wartungscenter 663–666
Microsoft Baseline Security Analyzer (MBSA) 617f.
Microsoft Data Protection Manager 88
Microsoft Deployment Toolkit (MDT) 72f.
Anwendungen hinzufügen 162ff.
Betriebssystemabbild hinzufügen 151f.
Distributionsfreigabe erstellen 150f.
Language Packs 162
LTI-Medien 165
Offlinedateien aktualisieren 161f.
SCCM, Integration 176f.
Tasksequenzen 153–160
Überblick 144–149
Updates hinzufügen 160f.
Verwalten und Verteilen von Abbildern, Überblick 149f.
Windows PE-Optionen, Konfigurieren 164
Microsoft Update, Anwendungswartung 124
Microsoft Virtual PC 263
Microsoft-Windows-Security-Licensing (SLC) 81
Migration
Benutzerprofildaten 34
Speichertypen 42
Übung mit Fallbeispiel, Migrieren von Benutzerdaten 49f.
Übung, Migrieren von Benutzerdaten 43ff.
von Windows Vista 26
von Windows XP 29f.
Windows-EasyTransfer 37ff.
MOBIKE 535
Mobile Computer *Siehe auch* Virtuelle private Netzwerke (VPN)
Freigegebene Ordner, konfigurieren 581
Offlinedateien 574–582
Synchronisierungscenter 579ff.
Transparente Zwischenspeicherung 577f.
Übung mit Fallbeispiel, Offlinedateien 596f.
Mobilität
Energiesparpläne 582–585, 587ff.
Freigegebene Ordner, konfigurieren 581
Offlinedateien 574–582
Synchronisierungscenter 579ff.
Transparente Zwischenspeicherung 577f.
Mobiltelefonnetz 358
Modems 401, 540–544
Module 673
Modus Verteilter Cache 460
MOF Generator, Assistent 703
MP3-Player 230ff.
MS-DOS-Stil, MBR-Partitionstabellen 234
Msinfo32 (Systeminformationen) 209f.
Multicast 330
Multifaktor-Authentifizierung 498
Multimediaeinstellungen 721
Multinet 327
Multiple Activation Key (MAK) 81

N

Nach Updates suchen 601
Nachbarcache 339
NAP (Network Access Protection) 536f., 610
NAT (Network Address Translation) 303, 335, 391, 401
Negative Zwischenspeicherung 312

Net share-Befehl 429f.
NetBIOS 308, 407
Netbook-Computer 6
Netsh
  BranchCache, Konfigurieren von Clients 461–466
  DirectAccess 518
  Drahtlosnetzwerke 349–354
  IPv4 konfigurieren 308
  IPv6 konfigurieren 338f.
  IPv6-zu-IPv4-Kompatibilität 335
  Übung, konfigurieren von DirectAccess 526f.
  Windows-Firewall 386
  Windows-Firewall mit erweiterter Sicherheit (WFAS) 393f.
Netstat 317ff., 336
Network Address Translation (NAT) 303, 335
Network Location Awareness (NLA) 383ff.
Netzwerk- und Freigabecenter
  Ad-hoc-Netzwerke 358
  Drahtlosnetzwerke 354
  Einwählverbindungen 540f.
  Erkennen der Netzwerkstandortkategorie 383
  Freigeben von Ressourcen 421f.
  Heimnetzgruppen 425
  ICS-Clients hinzufügen 305
  Internetverbindungen 347
  Verbindungen verwalten 360
  Virtuelle private Netzwerke (VPNs) 530
  Windows-Netzwerkdiagnose 313
Netzwerkadresse festlegen 421
Netzwerkadressübersetzung (NAT) 391, 401
Netzwerkbasierte Installation 97
Netzwerkbrücken 311, 361
Netzwerkdiagnose 678f.
Netzwerkdrucker hinzufügen, Assistent 367
Netzwerke *Siehe auch* Offlinedateien
  Ad-hoc-Netzwerke 358
  Auswählen des Netzwerktyps 13
  Drahtlos 678
  Drahtloscomputer hinzufügen 349–354
  Drahtlosnetzwerke
    Problembehandlung und Sicherheit 361–365
    Technologien 359
    Verwalten 354f.
  Drucken, Verbesserungen 367ff.
  Interne Drahtlosadapter, Sicherheit 355–358
  IPv4 konfigurieren
    Adressierung 298–305
    Problembehandlung 308–319
    Überblick 297f.
    Übung, Konfigurieren 319–323
    Verbindung mit Netzwerk herstellen 305–308
  IPv6 konfigurieren
    Adressen 326–331
    IPv4-Kompatibilität 332–335
    Konnektivität 336–340
    Übung, Konfigurieren von IPv6-Verbindungen 341ff.
    Vorteile von IPv6 331f.
  Konnektivität
    Überblick 345ff.
    Verbindungen einrichten 347ff.
    Verbindungen verwalten 360f.
Netzwerke *(Fortsetzung)*
  Leistungsüberwachung 719ff.
  Netzwerkdienste 302f.
  NLA (Network Location Awareness) 383ff.
  Übung mit Fallbeispiel
    Drahtlosnetzwerke 376f.
    IPv4-Verbindungen 376
    IPv6-Verbindungen 376
  Übung, Erstellen von Ad-hoc-Netzwerken 370ff.
  Verwalten 693
  Zonenregeln 274
Netzwerkfreigabe
  als Installationsquelle 8
  Aufzeichnen von Installationsabbildern 67f.
  Bereitstellung 68ff.
Netzwerksicherheitsschlüssel 353
Netzwerkzugriffsschutz (NAP) 536f., 610
Neue Anwendung, Assistent 163f.
Neue Sammlung erstellen, Assistent 657
Neue Tasksequenz, Assistent 174
Neuer Treiber, Assistent 152f.
Neustarts, überwachen 661f.
NFTS-Berechtigungen 430
NLA (Network Location Awareness) 383ff.
Notebooks *Siehe* Laptops
NTFS-Berechtigungen 440, 447, 556
NTFS-Dateien 165, 440, 447
NTLMv2 391
Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind 484

O

Objektrepository 699
OEM-Aktivierungslizenzen 81
Öffentliche Adressen 303ff.
Öffentliche Netzwerke 383
Offline Virtual Machine Servicing Tool 126, 161f.
Offline, dynamische Datenträger 238f.
Offlineabbilder 122, 127
Offlineangriffe 555
Offlinedateien 161f., 574–582, 596f., *siehe auch* Freigeben von Ressourcen
Offlineeinstellungen 428
Offline-Migrationen 42f.
offlineServicing 79
Offlinewebseiten 225ff.
Oktette 299
On/Off Transition Trace Capture Tool (Xbootmgr.exe) 723
Onlineabbilder bearbeiten 121f., 127
OOBE (Out-of-Box Experience) 93
oobeSystem 62, 79, 81
Optische Medien 170
Ordner
  Benutzerprofile wiederherstellen 773f.
  Beschädigte oder gelöschte Dateien wiederherstellen 768–774
  Datensicherungen 740–743
  Freigeben *Siehe auch* Virtuelle private Netzwerke (VPN)
    Bibliotheken 430
    BranchCache 459f.
    BranchCache, Konfigurieren von Clients 461–466
    BranchCache, Modus Gehosteter Cache 460

Ordner / Freigeben *(Fortsetzung)*
BranchCache, Modus Verteilter Cache 460f.
BranchCache, Windows Server 2008 466f.
Datei- und Ordnerberechtigungen 440–447
DirectAccess 526
Drucker 431ff.
Freigegebene Ordner 425–430
Netzwerk- und Freigabecenter 421f.
Offlinedateien 581
Überwachung konfigurieren 447ff.
Übung, BranchCache-Konfiguration 468f.
Übung, Freigeben von Ressourcen 433–437
Übung, Verschlüsselung und Berechtigungen 452–457
Übungen mit Fallbeispiel 472
Verschlüsselndes Dateisystem (EFS) 449–452
Migrieren von Benutzerprofildaten 34
Offlinedateien 574–582
Pfadregeln 272f., 280
Standard-Windows-Ordner 738
Übung
Konfigurieren einer Datei- und Ordnersicherung 745ff.
Migrieren von Benutzerdaten 43ff.
Wiederherstellen umbenannter Dateien 778–781
Übung mit Fallbeispiel, Migrieren von Benutzerdaten 49f.
User State Migration Tool (USMT) 39–42
Verwalten 693
Volumeschattenkopiedienst (VSS) 773
Wiederherstellen vorheriger Dateiversionen 772
Windows-EasyTransfer 35–39
Oscdimg 57
Out-of-Box Experience (OOBE) 93
Out-of-Box-Gerätetreiber 66, 121f.

P

Pakete 121, 129f., 133
Paketmanager (Pkgmgr.exe) 74, 116
Papierkorb 225ff., 772
Parameter, WIM2VHD 93f.
Partitionen
Basis- und dynamische Datenträger 234ff.
Datenträger, Benutzen 233f.
Netzwerkfreigabe, Bereitstellung 69
Passive Hubs 197
Patches 94, 124ff.
Pathping-Tool 313, 336
Peer Name Resolution-Protokoll (PNRP) 332, 404
Peer-to-Peer-Umgebungen 332
PEimg 74
Performance Analyzer 722
Personal Identification Number (PIN) 556f.
Personal-Modus 356ff.
Pfadregeln 270, 272f.
Phishing 628
Physikalischer Speicher 667
Physische Computer, Abbild bereitstellen 88
PIN (Personal Identification Number) 556f.
Ping 310–313, 315ff., 336
PIV-Standard 498
Pkgmgr.exe 74
Platzhalter 272f.
Plug & Play-Geräte (PnP) 80, 193–199
PnP *Siehe* Plug & Play-Geräte
PNRP *Siehe* Peer Name Resolution-Protokoll (PNRP)
Point-to-Point Tunneling Protocol (PPTP) 515, 530f., 535, 542
Popupblocker 633f.
Portable Computer
Einwählverbindungen 540f.
Energiesparpläne 582–585, 587ff.
Freigegebene Ordner, konfigurieren 581
Offlinedateien 574–582
Synchronisierungscenter 579ff.
Transparente Zwischenspeicherung 577f.
Übung mit Fallbeispiel, Offlinedateien 596f.
Verloren gegangene 555
Portbasierte Authentifizierung 356ff.
Ports 317ff., 385, 389
PowerShell 162, 406, 408, 411ff.
PPTP (Point-to-Point Tunneling Protocol) 515, 530f., 535, 542
Pre-Shared Key *Siehe* PSK-Modus (Pre-Shared Key)
Private Adressen 303ff.
Private Intranets 329f.
Private Netzwerke 303
Private Schlüssel 450
Problembehandlung
DirectAccess 519ff.
DirectX 213ff.
Drahtlosnetzwerke 361–365
Geräte-Manager 193
Gerätetreiber, Konflikte 209ff.
IP-Konfiguration 310–313
IPv4-Netzwerkkonnektivität 308–319
IPv6-Konnektivität 340
Programmkompatibilität 255
Richtlinien zur Anwendungskompatibilitätsdiagnose 262f.
Startkonfigurationsdaten 759f.
Übung mit Fallbeispiel, Leistung 730
Problembehandlung für Programmkompatibilität 255, 263
Problemgeräte 209
Process Explorer 264ff., 673ff.
Product Key 80f., 132
Programmdateien 278, 485f.
Programme und Funktionen 385
Protokollierung
Ereignisprotokollierung und -weiterleitung 676–684, 693, 730
Sysprep 82f.
Proxyserver 608
Prozessoren 5, 263
PSK-Modus (Pre-Shared Key) 356ff.
Public Key Encryption (Verschlüsselung mit öffentlichem Schlüssel) 450
Punkt-Dezimal-Notation 299f.
PXE-fähige Computer 170
PXE-kompatible Clients 145

Q

Quick Fix Engineering (QFE) 94

R

RADIUS (Remote Authentication Dial In User Service) 356ff.
RAID-5-Volumes 235, 237, 242ff.
RAM 263

RAM-Disk-Modus 134
Rechte
  Benutzerkontensteuerung (UAC)
    Einstellungen 478ff.
    Richtlinien 480–486
    Secpol und die Konsole Lokale Sicherheitsrichtlinie 486f.
    Übersicht 477f.
    Übung, konfigurieren 487ff.
  Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
  Virtuelle private Netzwerke (VPNs) 530
Referenzcomputer 58, 65f.
Regelbereich 390f.
Regelerstellungsassistent 280
Regeln 381, 383
Registrierung 485, 693, 734, 751–755
Remote Authentication Dial In User Service (RADIUS) 356ff.
RemoteApp 539f.
Remotecomputer, Geräte-Manager 194
Remotedesktop 400–403, 408ff., 496, 537–540
Remoteunterstützung 403ff.
Remoteverbindungen
  Einwählverbindungen 540–544
  Remotedesktop 537–540
  Überwachung 544
  Übung, konfigurieren von Remoteverbindungen 545ff.
  Übungen mit Fallbeispiel 551
  Virtuelle private Netzwerke (VPNs)
    Eingehende Verbindungen annehmen 542ff.
    NAP-Wartung 536f.
    Übersicht 530ff.
    VPN-Reconnect 535f.
Remoteverwaltung
  Remotedesktop 400–403
  Remoteunterstützung 403ff.
  Übung, Remoteverwaltungsoptionen 408–413
  Übungen mit Fallbeispiel 416
  Windows-Remoteverwaltung 406ff.
Ressourcen
  Auslastung überwachen 211
  Freigeben *Siehe auch* Virtuelle private Netzwerke (VPN)
    Bibliotheken 430
    BranchCache, Konfigurieren von Clients 461–466
    BranchCache, Modus Gehosteter Cache 460
    BranchCache, Modus Verteilter Cache 460f.
    BranchCache, Übersicht 459f.
    BranchCache, Windows Server 2008 466f.
    Datei- und Ordnerberechtigungen 440–447
    DirectAccess 526
    Drucker 431ff.
    Freigegebene Ordner 425–430
    Netzwerk- und Freigabecenter 421f.
    Überwachung konfigurieren 447ff.
    Übung, BranchCache-Konfiguration 468f.
    Übung, freigeben 433–437
    Übung, Verschlüsselung und Berechtigungen 452–457
    Übungen mit Fallbeispiel 472
    Verschlüsselndes Dateisystem (EFS) 449–452
  Geräte-Manager 197
  Hardware, Msinfo32 209
Ressourcen *(Fortsetzung)*
  Leistungsüberwachung und Berichterstellung
    CIM-Klassen 699f.
    Ereignisprotokollierung und -weiterleitung 676–684
    Leistungsoptionen 713ff.
    Netzwerkauslastung konfigurieren 719ff.
    Problembehandlung 717f.
    Process Explorer 673ff.
    Ressourcenmonitor 669–673
    Task-Manager 211, 718f.
    Überblick 651–661
    Übung, Leistungsüberwachung 684–690
    Übung, Windows-Leistungsanalysetools 723ff.
    Übungen mit Fallbeispiel 730f.
    Wartungscenter 663–666
    Windows Performance Toolkit (WPT) 721ff.
    WMI, CIMOM 698
    WMI, Überblick 693–697
    WMI-Anbieter 698
    WMI-Dienst 699
    WMI-Skriptingbibliothek 700
    WMI-Verbraucher 700
    WMI-Verwaltung 700–709
    Zuverlässigkeit, Stabilität und Leistung 661ff.
Ressourcenmonitor 669–673
Reverse-Lookup 332
RFM (Reduced Functionality Mode) 80
Richtlinie zum automatischen Hinzufügen 97, 102ff.
Richtlinien *Siehe auch* Gruppenrichtlinien
  AppLocker
    Konfigurieren von Ausnahmen 282
    Regeln 275–282
    Überwachung 283f.
    Übung, Beschränken von Anwendungen 284–288
  Automatisch hinzufügen 97, 102ff.
  Benutzerkontensteuerung (UAC) 480–486
  Benutzerrechte 496f.
  BitLocker To Go 564, 566
  BitLocker-DRAs 559f.
  BranchCache, Konfigurieren von Clients 461–466
  Datenträgerrichtlinien 230ff.
  DirectAccess 517–526
  Energieeinstellungen 587
  Ereignisabonnements 681f.
  Gerätetreiber 200f., 203f., 212, 216–222
  InPrivate 630f.
  IPSec 340
  Kontosperrungsrichtlinien 502
  Offlinedateien 576, 578
  Remotedesktopgateway 539
  Richtlinien für Softwareeinschränkung 269–275
  Richtlinien zur Anwendungskompatibilitätsdiagnose 262f.
  Schnellinfos 633
  Schreibcache konfigurieren 715f.
  Smartcards 498
  Standortabhängiges Drucken 368f.
  Überwachung von Remoteverbindungen 544
  Übungen
    BitLocker To Go 568–571
    Zugriffsrichtlinie und Konvertieren eines Datenträgers 246ff.

Richtlinien *(Fortsetzung)*
Übung mit Fallbeispiel
Beschränken von Anwendungen 292f.
Übung mit Fallbeispiel, Treibersignierung, Richtlinie 251
Updates 612
Windows Update 613ff.
Richtlinien für Softwareeinschränkung 254, 269–275, 284ff., 292f.
Richtlinien zur Anwendungskompatibilitätsdiagnose 262f.
RoboCopy.exe 447
Rollbacks 28, 612
Route, Befehlszeilentool 336
Router
Edgegeräte 391
SOHO, Windows-Firewall und 385
Standortlokale Adressen 329f.
Subnetze und Supernetze 300ff.
Umschalten zwischen WAPs 361f.
Rücksetzen von Benutzerkontenkennwörtern 500
Ruhezustand 400, 584, 723
Ruhezustandsdateien 225ff.
RunSynchronous 80

S

Sammlungssätze (DCS) 651, 654–661, 730
Saved Games-Ordner 738
ScanState 41
SCCM 2007 172–177
Schattenkopien 768–774
Schlüssel
Netzwerksicherheitsschlüssel 353
Startschlüssel 562
Verschlüsselung 556, 558
Wiederherstellungsschlüssel 560, 562
Windows-Firewall mit erweiterter Sicherheit (WFAS) 391
Schlüsselverwaltungsdienst (KMS) 81
Schnittstellen, IPv6 338f.
Schreiben
Benutzerkontensteuerungs (UAC) 485
Berechtigungen 440f.
Leistung 243
Schreibcache konfigurieren 715f.
Übung, Zugriff auf USB-Geräte 246f.
Wechseldatenträger, Richtlinien 232
Wechselmedien 230ff.
Schreibgeschützte Abbilder 118
Schriftarteinstellungen 130ff.
SCVMM (System Center Virtual Machine Manager) 95f., 126, 145, 161
Searches-Ordner 738
Secedit.exe 486f.
Secpol 486f.
Secure Socket Tunneling Protocol (SSTP) 515, 530, 535
Secure Sockets Layer (SSL) 627, 634–637
Security Health Validators (SHVs) 537
Security Template 486f.
Server Message Block (SMB) 174
Servergespeicherte Benutzerprofile 773
Service Set Identifier (SSID) 350f., 364f.
Setup Analysis Tool 261
Setupprotokolldateien 225ff.
Shim, Definition 259
SHVs (Security Health Validators) 537
Sicherer Desktop 482, 485
Sicherheit *Siehe auch* Remoteverwaltung; Updates; Benutzerkontensteuerung (UAC)
AppLocker
Konfigurieren von Ausnahmen 282
Regeln 275–282
Überwachung 283f.
Betriebssystemabbild hinzufügen 151
BitLocker
Aktivieren 561–564
BitLocker To Go 564, 566f.
Datenwiederherstellungsagenten (DRAs) 559ff.
Modi 556f.
TPM-Chip 558
Übersicht 555f.
Übung, BitLocker To Go 568–571
Datensicherung 741
Datenträgerrichtlinien 230ff.
DirectAccess 517ff.
Drahtlosnetzwerke 354, 364f.
Ereignisprotokollierung und -weiterleitung 676–684
Freigegebene Ressourcen
Datei- und Ordnerberechtigungen 440–447
Konfigurieren der Überwachung 447ff.
Übung, Verschlüsselung und Berechtigungen 452–457
Verschlüsselndes Dateisystem (EFS) 449–452
Gerätetreiber 201
Interne Drahtlosadapter 355–358
Internet Explorer, Einstellungen 624–627
Mobilität
Freigegebene Ordner, konfigurieren 581
Offlinedateien 574–582
Synchronisierungscenter 579ff.
Transparente Zwischenspeicherung 577f.
Übung mit Fallbeispiel, Offlinedateien 596f.
Netzwerkleistung 721
Netzwerksicherheitsschlüssel 353
Öffentliche und private Adressen 304
Patches, Offlineabbilder 126
Richtlinien für Softwareeinschränkung 269–275
SCCM 2007 172
Übung mit Fallbeispiel, Anwendungen beschränken 292f.
Übung, Beschränken von Anwendungen 284–288
Updates hinzufügen mit MDT 160f.
Verwalten 693
Virtuelle private Netzwerke (VPNs) 531–534, 537, 544
Vorabbereitstellen von Clientcomputern 103f.
Wartungscenter 663–666
Windows-Firewall 381–387, 394–397, 416
Windows-Firewall mit erweiterter Sicherheit (WFAS) 387–397, 416
Sicherheitscenter 537, 610
Sicherheitsstufen 270
Sichern und Wiederherstellen-Konsole
Datensicherungen planen 735–743
Eigene Dateien wiederherstellen 769
Systemabbildsicherungen 743ff.
Volumeschattenkopiedienst (VSS) 773
Sicherung *Siehe* Datensicherung

Side-by-Side-Migrationen 29
Signieren, Treiber 212–215
Sigverif (Dateisignaturverifizierung) 215
SIM *Siehe* Windows SIM (Windows System Image Manager)
SkipRearm 81
Skripts
  AppLocker, Skriptregeln 278
  Cscript 93
  Deployment Workbench 146
  Netzwerkfreigabe, Bereitstellung 69
  Regeln für 278
  Weitere Informationen 138
  WMI-Skriptingbibliothek 700
SKU (Stock-Keeping Unit, d.h. Edition) 3, 93
Small Office/Home Office (SOHO) 385
Smartcards 498f.
SmartScreen-Filter 627f.
SMS (System Management Server) 72
Snapshots 773
Software *Siehe* Anwendungen verwalten
SOHO-Netzwerk (Small Office/Home Office) 304f., 347ff., 356ff.
SOHO-Router (Small Office/Home Office) 385
specialize, Konfigurationsdurchlauf 79
Speicher *Siehe auch* Datenträger; Wechselmediengeräte; USB-Geräte (Universal Serial Bus)
  Dateibasiert 70
  Datensicherung 737, 740
  Defragmentieren von Datenträgern 227ff.
  ImageX 67f.
  Schreibcache konfigurieren 715f.
Speichersticks 715f.
Sperrungsrichtlinien, Konten 499f.
Split-WIM 94
Sprach-ID 137
SQL Server 145
SSID (Service Set Identifier) 350f., 364f.
SSL (Secure Sockets Layer) 627, 634–637
SSTP (Secure Socket Tunneling Protocol) 515, 530, 535
Stabilitätsdiagramm 663
Stabilitätsindex 662f.
Staging von Gerätetreibern 200f.
Standard User Analyzer 261
Standardanbieter 698
Standardgateway 301, 390
Standardregeln 270, 275f.
Standbymodus 723
Standortabhängiges Drucken 368f.
Standort-IDs 338
Standortlokale Adressen 329f.
Startabbilder
  WDS 73, 98, 100, 166f.
  Windows PE 116
Starten
  Startumgebung 567
  Startzeitfilterung 382
Startfähige Datenträger, Dual-Boot-Installationen 14–18
Startfähige Medien *Siehe auch* Systemstart
  Betriebssystempakete, Wartung 126–129
  LTI-Medien, Konfigurieren 165
  Suchabbilder 167f.
Startfähige Medien *(Fortsetzung)*
  Tasksequenz, Bereitstellen in VHD 157–160
  Übung, Erstellen von Windows PE-Start-DVD 83ff.
  VHD 89, 91f.
  WIM2VHD 93ff.
  Windows PE 66f.
  Windows-Startoptionen 759f.
Startkonfigurationsdaten (BCD) 759f.
Startschlüssel 562
Statistiken, Netzwerk 317ff.
Statusbehaftete Adresskonfiguration 329
Statusfreie Adresskonfiguration 329f.
Stealth 382
Stock-Keeping Unit (SKU) 3, 93
Störungen, Drahtlosverbindungen 362f.
Streaming, Multimedia 721
Stresstests, Gerätetreiber 211
Stripesetpartitionen 233, 235
Stripesetvolumes 237, 241–244
Stromverbrauch 196f.
Subnetzadresse 300
Subnetze 300ff.
Subnetzmasken 297
Suchabbild, WDS 74, 100, 167f.
Suchanbieter 631ff.
Supernetze 300ff.
Synchronisieren von Offlinedateien 574–582
Synchronisierungscenter 574, 579ff.
Sysprep 63, 76–83, 168
sysprep /generalize, Befehl 78
System aufräumen 77
System Center Virtual Machine Manager (SCVMM) 95f., 126, 145, 161
System Management Server (SMS) 72
System und Sicherheit 663–666, 735–743
System32, Windows-Ordner 485f.
Systemabbild, Datensicherung und -wiederherstellung 743ff., 754f.
Systemabbilder bereitstellen *Siehe auch* Systemabbilder konfigurieren
  Anwendungen, Wartung 124ff.
  Manuelle Installationen 177
  MDT (Microsoft Deployment Toolkit)
    Anwendungen hinzufügen 162ff.
    Betriebssystemabbild hinzufügen 151f.
    Distributionsfreigaben erstellen 150f.
    Gerätetreiber hinzufügen 152f.
    Language Packs 162
    LTI-Medien 165
    Offlinedateien aktualisieren 161f.
    Programmordner 146
    Tasksequenzen 153–160
    Überblick 144–149
    Updates hinzufügen 160f.
    Verwalten und Verteilen von Abbildern, Überblick 149f.
    Windows PE-Optionen 164
  Paketinstallation 129f.
  SCCM 2007 172–177
  Treiber, Wartung 122f.
  Übung, Herunterladen, Installieren und Konfigurieren von MDT 2010 177–183

Systemabbilder bereitstellen *(Fortsetzung)*
Übung, Offlineabbild bereitstellen und Language Packs installieren 139ff.
Übungen mit Fallbeispiel 187f.
Unbeaufsichtigte Wartung, Befehlszeile 135–138
WDS 165–172
WIM-Befehle, DISM 116–122
Windows PE-Abbilder, Wartung 133ff.
Windows-Editionen verwalten 132f.
Systemabbilder konfigurieren *Siehe auch* Systemabbilder bereitstellen
Betriebssystempakete, Wartung 126–129
DISM 74ff.
Internationale Einstellungen 130ff.
Offline Virtual Machine Servicing Tool 95f.
Referenzabbild erstellen 58–71
Sysprep 76–83
Überblick 53
Übung mit Fallbeispiel, Systemabbilder erstellen 110
Übung, Erstellen von startfähigen VHDs 104–107
Übung, WIM-Abbild erstellen 83ff.
Verteilen von Abbildern 71–74
VHDs, native 88–93
Vorabbereitstellen von Clientcomputern 102ff.
WDS, Online-VHD-Bereitstellung 96–104
WDS-Abbilder 73f.
WIM2VHD (Windows Image to Virtual Hard Disk) 93ff.
Windows Automated Installation Kit (Windows AIK) 55ff.
Windows Preinstallation Environment (WinPE) 57
Systembewertung 664ff.
Systemdateien, Datensicherung und -wiederherstellung 752
Systemeigenschaften 401, 404
Systemeinstellungen *Siehe* Einstellungen; Einstellungen, Netzwerk
Systemgebietsschema 130ff.
Systeminformationen (Msinfo32) 209f.
Systemintegritätsbericht 658–661
Systemmonitor 211
Systempartitionen, Netzwerkfreigabe, Bereitstellung 69
Systemprüfung für BitLocker 563
Systemstart *Siehe auch* Startfähige Medien
Bootmgr.exe 759f.
Leistung 721
Startoptionen 759f.
Überwachungsmodus oder Windows-Willkommensseite 81f.
Xbootmgr.exe 723
Zielcomputer 170f.
Systemwiederherstellung 756ff.
Startoptionen 759f.
Systemwiederherstellung 751–755
Übung, Computerschutz und Wiederherstellung 762–766
Vorversion wiederherstellen 761f.
Systemwiederherstellungs-Assistent 751f.
Systemwiederherstellungsoptionen 756ff.

T

Task-Manager 211, 718f.
Tasks
Anfügen an Ereignisse 678
Tasksequenz 146, 153–160
Verwalten 693
Tasksequenz-Editor 154, 174f.
Tastaturlayout 131f.
TCP/IP 678
Temporäre Dateien 225ff.
Teredo 333ff., 516, 519f.
Terminaldienste 537
Terminaldienstegateway 401, 537
Thick-Abbilder (vollständige) 148f., 151
Thin-Abbilder (partielle) 148–151
TLS (Transport Layer Security) 627
Tool zur Abbildverwaltung für die Bereitstellung *Siehe* DISM
TPM (Trusted Platform Module) 556ff., 564
Trace Capture, Processing, and Command-Line Analysis Tool (Xperf.exe) 722
Tracert-Tool 313, 336, 340
Transaktionsverarbeitung 144
Transmission Control Protocol/Internet Protocol (TCP/IP) 678
Transparente Zwischenspeicherung 577f.
Transport Layer Security (TLS) 627
Treiber, Geräte
Drucker freigeben 431
Hinzufügen, Microsoft Deployment Toolkit (MDT) 152f.
Informationen 121
Microsoft Deployment Toolkit (MDT) 144
Out-of-Box 66, 121f.
Plug & Play, beibehalten 80
Smartcards 498
Tastaturtreiber 131
Übung mit Fallbeispiel, Signierungsrichtlinie erzwingen 251
Updates 205
Vorversion wiederherstellen 761f.
Wartung 122f.
WIM-Abbilder 119
Windows PE-Abbilder 133
Treiberdetails 206
Treiberüberprüfungs-Manager 210f.
Tresor wiederherstellen 495
Troubleshooting *Siehe* Problembehandlung
Trusted Platform Module (TPM) 556ff., 564
Tzutil 132

U

UAC (Benutzerkontensteuerung)
Einstellungen 478ff.
Remoteunterstützung 403
Richtlinien 480–486
Secpol und die Konsole Lokale Sicherheitsrichtlinie 486f.
Übersicht 477f.
Übung mit Fallbeispiel, Benutzerkontensteuerung und Kennwörter 511f.
Übung, konfigurieren 487ff.
Übergreifende Partitionen 233, 235
Übergreifende Volumes 237, 240f.
Überlappende Netzwerke 362
Überprüfung 64, 201
Überwachen von Systemen
Dienste-Konsole 711ff.
Ereignisprotokollierung und -weiterleitung 676–684
Leistungsüberwachung und Berichterstellung 651–661
CIM-Klassen 699f.
CIMOM 698

Überwachen von Systemen / Leistungsüberwachung und Berichterstellung *(Fortsetzung)*
CIM-Repository 699
Leistungsoptionen 713ff.
Netzwerkauslastung konfigurieren 719ff.
Problembehandlung 717f.
Schreibcache konfigurieren 715f.
Übung, Leistungsüberwachung 684–690
Übung, Windows-Leistungsanalysetools 723ff.
Übungen mit Fallbeispiel 730f.
Windows Performance Toolkit (WPT) 721ff.
WMI, Überblick 693–697
WMI-Anbieter 698
WMI-Dienst 699
WMI-Skriptingbibliothek 700
WMI-Verbraucher 700
WMI-Verwaltung 700–709
Process Explorer 673ff.
Ressourcenmonitor 669–673
Task-Manager 211, 718f.
Wartungscenter 663–666
Zuverlässigkeit, Stabilität und Leistung 661ff.
Überwachung
AppLocker 283f.
auditSystem, Konfigurationsdurchlauf 79
auditUser, Konfigurationsdurchlauf 79f.
Freigegebene Ressourcen 447ff.
Remoteverbindungen 544
Sicherheitsereignisprotokoll 676–684
Überwachungsmodus, Starten 81f.
Übungen
Aktualisieren auf Windows 7 30f.
Anmeldeinformationen, verwalten 504–507
Benutzerkontensteuerung (UAC), konfigurieren 487ff.
BitLocker To Go 568–571
BranchCache-Konfiguration 468f.
Computerschutz und Wiederherstellung 762–766
Datensicherung, Konfigurieren einer Datei- und Ordnersicherung 745ff.
Datenträger, Zugriffsrichtlinie und Konvertieren 246ff.
DirectAccess, mit Netsh konfigurieren 526f.
Durchführen einer Neuinstallation 18–21
Energiesparpläne verwalten 589–592
Freigeben von Ressourcen 433–437
Freigegebene Ressourcen, Verschlüsselung und Berechtigungen 452–457
Gerätetreiber, Konfigurieren von Richtlinien und Treibersuche 216–222
Internet Explorer, InPrivate-Modus und Add-Ons 637–641
Kompatibilität 264ff.
Leistungsüberwachung 684–690
MDT 2010, Herunterladen, Installieren und Konfigurieren 177–183
Migrieren von Benutzerdaten 43ff.
Offlineabbild bereitstellen und Language Packs installieren 139ff.
Remoteverbindungen, konfigurieren von 545ff.
Remoteverwaltungsoptionen 408–413
VHD, startfähig 104–107
Wiederherstellen umbenannter Dateien 778–781
WIM-Abbild erstellen 83ff.
Übungen *(Fortsetzung)*
Windows Update, konfigurieren 618ff.
Windows-Firewall 394–397
Windows-Leistungsanalysetools 723ff.
Übungen mit Fallbeispiel
Anwendungen beschränken 292f.
Anwendungskompatibilität 292
Benutzerkontensteuerung (UAC) 511
Bereitstellen eines Abbilds 187f.
Datensicherung und -wiederherstellung 785
Drahtlosnetzwerke 376f.
Freigegebene Ressourcen 472
Installieren von Windows 7 49
Internet Explorer 646f.
IPv4-Verbindungen 376
IPv6-Verbindungen 376
Kennwörter, Problembehandlung 511f.
Leistungsüberwachung 730f.
Offlinedateien 596f.
Remoteverwaltung 416
Remotezugriff 551
System- und Konfigurationsprobleme 785f.
Systemabbild erstellen 110
Treibersignierung, Richtlinie 251
Verwalten von Datenträgervolumes 251
VHDs benutzen 110
Windows-Firewall 416
UDP (User Datagram Protocol) 333
UIAccess-Anwendungen 485f.
UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern 485
Unattend.xml-Antwortdateien 93, 126, 135–138
Unbeaufsichtigte Installationen 59, 79f., 82
Universal Serial Bus-Geräte (USB)
als Installationsquelle 6f.
BitLocker 563f.
Datensicherungsziel 740
Defragmentieren 227ff.
Einwählverbindungen 540f.
Kennwortrücksetzdatenträger 500
Netzwerkverbindungen 347ff.
Richtlinien 230ff.
Schreibcache konfigurieren 715f.
Sicherheit und 555
Suchabbilder 167f.
Systemstart, Laufwerke 170
Übung, Schreibzugriff 246f.
Verschlüsselndes Dateisystem (EFS) 449
Unspezifizierte Adresse 330
Updates
Abbilder, WDS 102
Anwendungen, Wartung 124ff.
Gerätetreiber 193, 204
Hinzufügen, MDT (Microsoft Deployment Toolkit) 160f.
Microsoft Baseline Security Analyzer (MBSA) 617f.
Offline Virtual Machine Servicing Tool 95
Offlinedateien 161f.
SCCM 2007 172
Übung, konfigurieren von Windows Update 618ff.
Übungen mit Fallbeispiel 646
Wartungscenter 609f.

Updates *(Fortsetzung)*
WIM-Abbilder 119
Windows Server Update Services (WSUS) 610–613
Anwendungswartung 124
NAP-Wartung 537
Offline Virtual Machine Servicing Tool 95
Offlinedateien 161
Windows Update
Gerätetreiber installieren 200f.
Konfigurieren von 601–609
Richtlinien 613ff.
Smartcards 498
Übung mit Fallbeispiel 646
Übung, konfigurieren 618ff.
Wartungscenter 663–666
Zuverlässigkeit, Stabilität und Leistung 661ff.
Updateverlauf anzeigen 604
Upgrades
Übung, Aktualisieren auf Windows 7 30f.
von Windows 7-Editionen 25f.
von Windows Vista 26ff.
USB-Controller 198, 347ff.
USB-Geräte (Universal Serial Bus)
als Installationsquelle 6f.
BitLocker 563f.
Datensicherungsziel 740
Datenträgerrichtlinien 230ff.
Defragmentieren 227ff.
Einwählverbindungen 540f.
Kennwortrücksetzdatenträger 500
Schreibcache konfigurieren 715f.
Sicherheit und 555
Suchabbilder 167f.
Systemstart, Laufwerke 170
Übung, Schreibzugriff 246f.
Verschlüsselndes Dateisystem (EFS) 449
USB-Hubs, Stromverbrauch 197
User Account Control *Siehe* Benutzerkontensteuerung (UAC)
User Datagram Protocol (UDP) 333
User Interface Accessibility (UIAccess) 485
User State Migration Tool (USMT) 39–42, 55ff.

V

Verbinden mit bevorzugtem Netzwerk 362
Verbindungen *Siehe auch* Remoteverwaltung; Windows-Firewall
DirectAccess
Clientkonfiguration 517–521
Problembehandlung 519ff.
Server konfigurieren 521–526
Übersicht 515ff.
Übung, mit Netsh konfigurieren 526f.
Remote
Eingehende Verbindungen annehmen 542ff.
Einwählverbindungen 540f.
NAP-Wartung 536f.
Remotedesktop 537–540
Überwachung 544
Übung, konfigurieren von Remoteverbindungen 545ff.
Übungen mit Fallbeispiel 551
Virtuelle private Netzwerke (VPNs) 530ff.
VPN-Reconnect 535f.
Verbindungen *(Fortsetzung)*
Statistiken 317ff.
Windows-Firewall mit erweiterter Sicherheit (WFAS) 391ff.
Verbindungslokale Adressen 329f.
Verbrauch, Strom 197
Vererben von Berechtigungen 444, 446f.
Verfügbarkeit 242ff.
Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus 481
Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer 483
Verschieben von Dateien 446f.
Verschlüsselndes Dateisystem (EFS) 449–452, 493, 500, 502ff., 556, *siehe auch* Verschlüsselung
Verschlüsselung *Siehe auch* Verschlüsselndes Dateisystem (EFS)
BitLocker
Aktivieren 561–564
BitLocker To Go 564, 566f.
Datenwiederherstellungsagenten (DRAs) 559ff.
Modi 556f.
TPM-Chip 558
Übersicht 555f.
Übung, BitLocker To Go 568–571
Datensicherung 734
Ereignisweiterleitung 679
Freigegebene Ressourcen
Übung, Verschlüsselung und Berechtigungen 452–457
Übungen mit Fallbeispiel 472
Interne Drahtlosadapter 355–358
Netzwerksicherheitsschlüssel 353
SSL-Zertifikate konfigurieren 634–637
Virtuelle private Netzwerke (VPNs) 531f.
Wiederherstellungsagenten 451f.
Windows-Firewall mit erweiterter Sicherheit (WFAS) 391ff.
Verschlüsselung mit öffentlichem Schlüssel (Public Key Encryption) 450
Vertrauen 407
Vertrauenswürdige Herausgeber, Zertifikatspeicher 212–215
Vertrauenswürdige Sites 274
Vertrauenswürdige Stammzertifizierungsstelle 213
Verwaiste Abbilder 120
Verwalten
Anwendungen
Application Compatibility Toolkit (ACT) 258–262
AppLocker, Konfigurieren von Ausnahmen 282
AppLocker, Überwachung 283f.
AppLocker-Regeln 275–282
AppLocker-Richtlinien, Überblick 275
Ausführbare Regeln 276
Kompatibilität, konfigurieren 255–258
Richtlinien für Softwareeinschränkung 269–275
Richtlinien zur Anwendungskompatibilitätsdiagnose 262f.
Übersicht 253
Übung, Beschränken von Anwendungen 284–288
Übung, Kompatibilität 264ff.
Übungen mit Fallbeispiel 292f.
Windows XP Mode 263f.
Benutzerkontensteuerung (UAC) 477f., 480–489

Verwalten *(Fortsetzung)*
Benutzerprofile
Migrieren von Benutzerprofildaten 34
Übung, Migrieren von Benutzerdaten 43ff.
User State Migration Tool (USMT) 39–42
Windows-EasyTransfer 35–39
BitLocker
Aktivieren 561–564
BitLocker To Go 564, 566f.
Datenwiederherstellungsagenten (DRAs) 559ff.
Modi 556f.
TPM-Chip 558
Übersicht 555f.
Übung, BitLocker To Go 568–571
Datenträger
Basis- und dynamische Datenträger 234ff.
Datenträgervolumes 239–245
Partitionen benutzen 233f.
Reaktivieren dynamischer Datenträger 238f.
Übung mit Fallbeispiel, Verwalten von Datenträgervolumes 251
Übung, Konfigurieren von Richtlinien und Konvertieren von Datenträgern 246ff.
Verschieben 237f.
Wartung 225–232
DirectAccess
Clientkonfiguration 517–521
Problembehandlung 519ff.
Server konfigurieren 521–526
Übersicht 515ff.
Übung, mit Netsh konfigurieren 526f.
Übungen mit Fallbeispiel 551
Drahtlosnetzwerke 354f.
Drucker 433
Freigegebene Ressourcen
BranchCache 459f.
BranchCache, Konfigurieren von Clients 461–466
BranchCache, Modus Gehosteter Cache 460
BranchCache, Modus Verteilter Cache 460f.
BranchCache, Windows Server 2008 466f.
Ordner 429f.
Übung, BranchCache-Konfiguration 468f.
Geräte
Benutzen mit Treiber 204ff.
Dateisignaturverifizierung 215
Geräte-Manager 193–199
Installieren, Windows Update 200f.
Konfigurieren von Installationsrichtlinien 203f.
Konflikte beseitigen 207–210
Nicht-PnP-Geräte installieren 202
Staging von Gerätetreibern 200f.
Treibersignierung und digitale Signaturen 212–215
Treiberüberprüfungs-Manager 210f.
Überblick 199
Übung, Konfigurieren von Richtlinien und Treibersuche 216–222
Internet Explorer, InPrivate-Modus 628–631
Leistung
CIM-Klassen 699f.
CIM-Repository 699
WMI, CIMOM 698
Verwalten / Leistung *(Fortsetzung)*
WMI, Überblick 693–697
WMI-Anbieter 698
WMI-Dienst 699
WMI-Skriptingbibliothek 700
WMI-Verbraucher 700
WMI-Verwaltung 700–709
Netzwerkverbindungen 360f.
Remoteverwaltung
BCDEdit 759f.
Remotedesktop 400–403
Remoteunterstützung 403ff.
Übung, Remoteverwaltungsoptionen 408–413
Übungen mit Fallbeispiel 416
Windows-Remoteverwaltung 406ff.
Systemabbild bereitstellen
Anwendungen hinzufügen 162ff.
Anwendungen, Wartung 124ff.
Betriebssystemabbild hinzufügen 151f.
Betriebssystempakete, Wartung 126–129
Distributionsfreigabe erstellen 150f.
Gerätetreiber hinzufügen 152f.
Internationale Einstellungen 130ff.
Language Packs 162
LTI-Medien 165
Manuelle Installationen 177
MDT (Microsoft Deployment Toolkit), Überblick 144–149
Offlinedateien aktualisieren 161f.
Paketinstallation 129f.
SCCM 2007 172–177
Tasksequenzen 153–160
Treiber, Wartung 122f.
Übung, Herunterladen, Installieren und Konfigurieren von MDT 2010 177–183
Übung, Offlineabbild bereitstellen und Language Packs installieren 139ff.
Übungen mit Fallbeispiel 187f.
Unbeaufsichtigte Wartung, Befehlszeile 135–138
Updates hinzufügen 160f.
Verwalten und Verteilen von Abbildern, Überblick 149f.
WDS 165–172
WIM-Befehle, DISM 116–122
Windows PE 133ff., 164
Windows-Editionen verwalten 132f.
Übung, Verwalten von Anmeldeinformationen 504–507
Virtuelle Festplatten
Native VHDs benutzen 88–93
Offline Virtual Machine Servicing Tool 95f.
Übung mit Fallbeispiel, VHDs benutzen 110
Übung, Erstellen von startfähigen VHDs 104–107
Vorabbereitstellen von Clientcomputern 102ff.
WDS, Online-VHD-Bereitstellung 96–104
WIM2VHD (Windows Image to Virtual Hard Disk) 93ff.
Windows-Firewall 381–387, 394–397
Windows-Firewall mit erweiterter Sicherheit (WFAS)
Übersicht 387–394
Übung, konfigurieren 394–397
Zertifikate 502ff.
VHD *Siehe* Virtuelle Festplatten (VHDs)
Virtual PC 88f.
Virtual Server 88f.

Virtuelle Computer, Abbild bereitstellen 88
Virtuelle Festplatten (VHDs)
Abbild erstellen, Windows PE 66
Anfügen und trennen 90
Betriebssystempakete, Wartung 126–129
BitLocker-Wiederherstellung 567
Datensicherungsziel 740
Defragmentieren 227ff.
Dual-Boot-Installationen 16ff.
LTI-Medien 165
Native, benutzen 88–93
Netzwerkfreigabe, Abbild speichern 67f.
Offline Virtual Machine Servicing Tool 95f.
Offlinedateien aktualisieren 161f.
Starteintrag, Hinzufügen 92f.
Systemabbildsicherungen 743ff.
Systemstart 91f.
Tasksequenz, Bereitstellen in VHD 157–160
Übersicht 513
Übung mit Fallbeispiel, VHDs benutzen 110
Übung, Erstellen von startfähigen VHDs 104–107
Updates 53
Vorabbereitstellen von Clientcomputern 102ff.
WDS, Online-VHD-Bereitstellung 96–104
WIM2VHD 93ff.
Virtuelle private Netzwerke (VPN)
Authentifizierungsprotokolle 533f.
DirectAccess
Clientkonfiguration 517–521
Problembehandlung 519ff.
Server konfigurieren 521–526
Übersicht 515ff.
Übung, mit Netsh konfigurieren 526f.
Drahtlosnetzwerke 354
Eingehende Verbindungen annehmen 542ff.
NAP-Wartung 536f.
Remotedesktopverbindungen 401
Übersicht 530ff.
Überwachung 544
Übung, konfigurieren von Remoteverbindungen 545ff.
Übungen mit Fallbeispiel 551
VPN-Reconnect 535f.
Visual Trace Analysis Tool (Xperfview.exe) 722
Visuelle Effekte 713f.
Vollqualifizierte Domänennamen (FQDNs) 407
Vollständige Wiederherstellung 754f.
Volumenlizenzen 81
Volumes, Datenträger
Größe ändern 244f.
Löschen 245
Übung mit Fallbeispiel, Verwalten 251
Verwalten 239–245
Volumeschattenkopiedienst (VSS) 773
Volumestatus 237
Vorinstallierte Schlüssel (PSK) 356ff.
Vorlagendateien
Deployment Workbench 146
Security Template 486f.
Vorrang 270, 272f.
Vorschaubilder 225ff.
Vorversion wiederherstellen 204
VPN (virtuelle Private Netzwerke) *Siehe* Virtuelle private Netzwerke (VPN)
VPN-Reconnect 535f.
VSS (Volumeschattenkopiedienst) 773

W

WAN (Wide Area Network) 346, 577
WAP (Wireless Access Point) 302f., 305, 309, 361f.
Warnungen, Leistungsindikatoren 656
Wartungsaufgaben, Datenträger 225–232
Wartungsaufträge 162
Wartungscenter 609f., 663–666
Wbadmin 743
WCS (Windows Color System) 367
WDS (Windows Deployment Services)
Abbild bereitstellen 151, 165–172
als Installationsquelle 8f.
MMC-Snap-In
Abbilder 73f.
Aktualisieren eines Abbilds 102
Aufzeichnungsabbild erstellen 99
Exportieren von Abbildern 101
Installationsabbild hinzufügen 100f.
Startabbild hinzufügen 100
Suchabbild erstellen 100
Überblick 97
Online-VHD-Bereitstellung 96–104
WDSUTIL 97, 102ff., 171f.
Web Proxy Auto Detect (WPAD) 608
Websites, Zertifikatfehler 636
Wechselmediengeräte *Siehe auch* USB-Geräte (Universal Serial Bus)
Datenlaufwerke 566
Datenträgerrichtlinien 230ff.
Partionieren 234
Systemstart, Laufwerke 170
Übung, Schreibzugriff 246f.
Weitere Informationen
Abbilder erstellen 74
ACT 258, 262
Antwortdateien 64, 80
AppLocker-Überwachung 284
BCDBoot 70, 171
BCDEdit 93
BCD-Startoptionen 760
BCD-WMI-Schnittstelle 760
Benutzerdefinierte Befehle und Skripts hinzufügen 138
Bereitstellung 66, 98
Biometrie 498
BitLocker 556
BitLocker-DRAs 561
Bluetooth 353
BranchCache-Server, Konfigurieren 460
DirectAccess 516, 519, 521
Diskpart 170, 245
Distributed Management Task Force (DMTF) 700
Druckerberechtigungen 433
EAP 357
Eigenständiges Windows Update-Installationsprogramm 609
El Torito-Startsektordatei 67
Energieverwaltung 585

Weitere Informationen *(Fortsetzung)*
Erweiterte Systemtools und Befehlszeilenprogramme 674
Erweiterte Überwachungsrichtlinien 449
Erzwingen der Treibersignatur deaktivieren 213
Externe Auflösung 347
Freigabeberechtigungen und NTFS-Berechtigungen 430
Gemeinsame Nutzung der Internetverbindung 305
Globale Unicastadressen 328
Icacls 445
Interne und externe Auflösung 303
Internet Explorer, erweiterte Sicherheit 627
Ioctl_disk_performance-Datei 684
IPv6-Adressierung 328
Konfigurationsdurchlauf 138
LoadState 41
Logman 658
Lokale Standardbenutzergruppen 497
MDT (Microsoft Deployment Toolkit) 146
Microsoft Baseline Security Analyzer (MBSA) 618
Microsoft-Windows-Security-Licensing-SLC 81
Migration 40, 42f.
MOF-Dateien kompilieren 706
NAP 537
Netsh 339
Network Address Translation (NAT) 303
Netzwerkbrücken 311
Offline Virtual Machine Servicing Tool und SCVMM 162
Peer Name Resolution-Protokoll 332
Physikalischer Datenträger, Zeit (%), Leistungsindikator 687
PnPUtil 221
Powercfg.exe 588
RemoteApp 540
Remotedesktopgateway 538
Remotezugriff, Windows PowerShell 408
Richtlinien für Softwareeinschränkung 274
Sammlungssätze 657
ScanState 41
SCCM 2007 und Softwareupdates 177, 611
SCCM-Clientsuche 173
Smartcards 499
Subnetzunterteilung und Supernetze 301
Sysprep, Überwachungsmodus 78
Tasksequenzaktionen und -variablen 175
Tasksequenz-Editor 157
TCP-Verbindungsstatus 319
Teredo-Adressen 335
Transparente Zwischenspeicherung 578
Treiberspeicher und Staging 201
Treiberüberprüfungs-Manager 211
Überwachungsmodus und Sysprep 63
Überwachungsmodus, Starten 82
Umleiten von Dateien und Einstellungen 41
USMT 57
Verschlüsselndes Dateisystem (EFS) 450
Verwalten von Abbildern mit WDS 102
VIM2VHD 95
Virtual PC und Windows XP 740
Virtuelle Festplatten (VHDs) 89
Vorabbereitstellen von Clientcomputern 103f.
Wbadmin 744
WDS 97ff., 172
Weitere Informationen *(Fortsetzung)*
WDSUTIL 172
Web Proxy Auto Detect 608
Windows 7 Upgrade Advisor 27
Windows 7-Bereitstellung 70
Windows-Abbild, Status 82
WMI-Klassen 695
WSUS 613
WEP (Wireless Equivalent Privacy) 355ff.
WFAS *Siehe* Windows-Firewall mit erweiterter Sicherheit (WFAS)
Wide Area Network (WAN) 346, 577
Wiederherstellen 493ff., 751–755, 764, 768–774
Wiederherstellung, Daten *Siehe auch* Datensicherung
Benutzerprofile wiederherstellen 773f.
Beschädigte oder gelöschte Dateien wiederherstellen 768–774
Computerschutz und Datenträgernutzung konfigurieren 776f.
Datei kopieren 734
Erweiterte Startoptionen 756ff.
Startoptionen 759f.
Übung, Wiederherstellen umbenannter Dateien 778–781
Übungen mit Fallbeispiel 785f.
Umbenannte und gelöschte Dateien 772
Volumeschattenkopiedienst (VSS) 773
von BitLocker-geschützten Laufwerken 566f.
Vorgängerversionen von Dateien 772
Wiederherstellung, System 761–766
Wiederherstellungsagenten 451f.
Wiederherstellungseinstellungen 776
Wiederherstellungskennwörter 559f.
Wiederherstellungsschlüssel 560, 562
Wi-Fi Protected Access (WPA) 355–358
WIM (Windows Imaging)
Abbild bereitstellen 116–122
Abbildformat 70f.
Befehlsoptionen 75
Bereitgestellte Abbilder, Informationen 119f.
Übung, WIM-Abbild erstellen 83ff.
WIM2VHD (Windows Image to Virtual Hard Disk) 93ff.
Wimscript.ini 67, 70
Windows 7
Aktivierung zurücksetzen 80f.
Aktualisieren von Windows 7-Editionen 25f.
Aktualisieren von Windows Vista 26ff.
Automatische Installation, Windows AIK 55ff.
Editionen, Überblick 3
Enterprise 4f., 91, 95, 275, 401, 449, 459, 517, 564, 574
Hardwarevoraussetzungen 5
Home Basic 4
Home Premium 4
Installationsquelle vorbereiten 6–9
Installieren von 9–18
Migrieren von Windows XP 29, 30
Professional 401, 449, 574
Starter 3
Übung, Aktualisieren auf Windows 7 30f.
Übung, Durchführen einer Neuinstallation 18–21
Ultimate 4f., 91, 95, 275, 401, 449, 459, 517, 564, 574
Windows 7 Professional 4

Windows 7 Upgrade Advisor 27
Windows AIK (Windows Automated Installation Kit)
  BCDboot 170
  Bereitstellen von Abbildern im Dateisystem 116
  Installieren und benutzen 55ff.
  Übung, Installieren 83ff.
  USMT (User State Migration Tool) 39–42
  VHDs, native 89
Windows Color System (WCS) 367
Windows Deployment Services *Siehe* WDS (Windows Deployment Services)
Windows Imaging (WIM)
  Abbild bereitstellen 116–122
  Abbildformat 70f.
  Befehlsoptionen 75
  Bereitgestellte Abbilder, Informationen 119f.
  Übung, WIM-Abbild erstellen 83ff.
Windows Installer (.msi) 122, 124ff., 274, 277
Windows Internet Naming Service (WINS) 308, 390
Windows PE
  Abbilder erstellen 55ff.
  Abbilder, Wartung 133ff.
  Aufzeichnungsabbild, WDS 73
  Featureeinstellungen 62
  Konfigurationsdurchläufe 79
  Konfigurieren von Optionen 164
  Netzwerkfreigabe, Abbild speichern 67f.
  Profilerstellungstool 134
  Startabbilder 116
  Startfähige Medien erstellen 66f.
  Systemabbilder aufzeichnen 57
  Übung, Erstellen von Start-DVD 83ff.
  Windows AIK-Tools 57
Windows Performance Toolkit (WPT) 721ff.
Windows PowerShell 162, 406, 408, 411ff.
Windows Preinstallation Environment (WinPE) *Siehe* Windows PE
Windows RE (Wiederherstellungsumgebung) 754f., 758
Windows Recovery Environment *Siehe* Windows-Wiederherstellungsumgebung (Windows RE)
Windows Server 2003 95, 172, 269–275, 459
Windows Server 2008
  Abwärtskompatibilität 116
  Änderungs- und Konfigurationsverwaltung 172
  BranchCache 459, 466f.
  DirectAccess 522
  MDT (Microsoft Deployment Toolkit) 72
  Offline Virtual Machine Servicing Tool 95
  Remotedesktop 401
  Remoteunterstützung 404
  Richtlinien für Softwareeinschränkung 269–275
  Suchabbild erstellen 168
  Teredo-Adresse 333ff.
Windows Server und Zertifikatdienste 212–215
Windows Server Update Services (WSUS)
  Anwendungswartung 124
  NAP-Wartung 537
  Offline Virtual Machine Servicing Tool 95
  Offlinedateien 161
  Übersicht 610–613
Windows Server-Sicherung 88
Windows SIM (System Image Manager) 57ff., 80, 136f.
Windows System Image Manager *Siehe* Windows SIM (Windows System Image Manager)
Windows Update
  Gerätetreiber installieren 200f.
  Konfigurieren von 601–609
  Richtlinien 613ff.
  Smartcards 498
  Übung mit Fallbeispiel 646
  Übung, konfigurieren 618ff.
  Wartungscenter 663–666
Windows Update Stand-alone Installer (.msu) 126f.
Windows Virtual PC 385, 739
Windows Vista
  Abwärtskompatibilität 116
  Aktualisieren von 26ff.
  Bereitstellen in VHD 157–160
  BitLocker 564
  DirectAccess 517
  Migrieren von Benutzerprofildaten 34, 39
  Remotedesktop 401
  Remoteunterstützung 404
  Richtlinien für Softwareeinschränkung 269–275
  Teredo-Adresse 333ff.
  Übung, Aktualisieren auf Windows 7 30f.
  Verbindungssicherheit und IPSec 393
  Windows-EasyTransfer 35–39
  Windows-Firewall 383, 385
Windows XP
  DirectAccess 517
  Migration von 29f.
  Migrieren von Benutzerprofildaten 34, 39
  Remotedesktop 401
  Remoteunterstützung 403ff.
  Richtlinien für Softwareeinschränkung 269–275
  ScanState 41
  Verbindungssicherheit und IPSec 393
  Windows XP Mode 263f.
  Windows-EasyTransfer 35–39
Windows-Aufgabenplanung 744
Windows-Bereitstellung, Assistent 165
Windows-Bereitstellungsdienste (WDS)
  als Installationsquelle 8f.
  Assistent zur Abbildaufzeichnung 73, 169
  MMC-Snap-In
    Abbilder 73f.
    Aktualisieren eines Abbilds 102
    Aufzeichnungsabbild erstellen 99
    Exportieren von Abbildern 101
    Installationsabbild hinzufügen 100f.
    Startabbild hinzufügen 100
    Suchabbild erstellen 100
    Überblick 97
  Online-VHD-Bereitstellung 96–104
Windows-Bereitstellungstools 89
Windows-Betriebssystemladeprogramm (Winload.exe) 759f.
Windows-DDNS 330
Windows-Ereignissammlung 679
Windows-Firewall
  Ereignisweiterleitung 679
  Netzwerkeinstellungen konfigurieren 315ff.

Windows-Firewall *(Fortsetzung)*
NLA (Network Location Awareness) 383ff.
Ping-Befehle 339
Programme zulassen 385f.
Übersicht 381–387
Übung mit Fallbeispiel 416
Übung, konfigurieren 394–397
Windows-Firewall mit erweiterter Sicherheit (WFAS) 315ff.
DirectAccess 526
Netzwerkeinstellungen konfigurieren 315ff.
Übersicht 387–394
Übung mit Fallbeispiel 416
Übung, konfigurieren 394–397
Windows-Fortsetzungsladeprogramm (Winresume.exe) 759f.
WindowsImageBackup-Ordner 744f.
Windows-Leistungsanalysetoolkit *Siehe* Windows Performance Toolkit (WPT)
Windows-Leistungsindex 664ff.
Windows-Netzwerkdiagnose-Tool 313f., 678f.
Windows-Ordner 278, 485
Windows-Remoteshell (WinRS) 393, 407f., 411ff.
Windows-Remoteunterstützung 403ff., 485
Windows-Remoteverwaltung (WinRM) 406ff., 679f.
Windows-Setup 78
Windows-Start-Manager (Bootmgr.exe) 759f.
Windows-Tresor 493ff.
Windows-Vorinstallationsumgebung *Siehe* Windows PE
Windows-Wiederherstellungsumgebung (Windows RE) 754f., 758
Windows-Willkommensseite 63, 81f.
Winload.exe 759f.
WinPE (Windows Preinstallation Environment)
Abbilder erstellen 55ff.
Aufzeichnungsabbild, WDS 73
Featureeinstellungen 62
Konfigurationsdurchläufe 79
Konfigurieren von Optionen 164
Netzwerkfreigabe, Abbild speichern 67f.
Profilerstellungstool 134
Startabbilder 116
Startfähige Medien erstellen 66f.
Systemabbilder aufzeichnen 57
Übung, Erstellen von Start-DVD 83ff.
Windows AIK-Tools 57
Winresume.exe 759f.
WinRM (Windows-Remoteverwaltung) 406, 679f.
WinRS (Windows Remote Shell) 393, 406ff., 411ff.
WINS *Siehe* Windows Internet Naming Service (WINS)
Wipe-and-Load-Migrationen 30
Wired Equivalent Privacy (WEP) 355ff.
Wireless Access Point *Siehe* WAP (Wireless Access Point)
WMI
Anbieter 697
CIM-Klassen 699f.
CIM-Repository 699
CIM-Studio 700–703
Dienst 697
Ereignisanzeige 707ff.
Ereignisregistrierung 706f.
Objektbrowser 703ff.
Repository 697
WMI *(Fortsetzung)*
Überblick 693–697
WMI-Anbieter 698
WMI-Dienst 699
WMI-Skriptingbibliothek 700
WMI-Verbraucher 700
WMI-Verwaltung 700–709
WPA2-Enterprise 357
WPA2-Zertifizierungen 356ff.
WPAD (Web Proxy Auto Detect) 608
WPA-Enterprise 357
WPT (Windows Performance Toolkit) 721ff.
WQL Query Builder 703
WSUS (Windows Server Update Services) 610–613
Anwendungswartung 124
NAP-Wartung 537
Offline Virtual Machine Servicing Tool 95
Offlinedateien aktualisieren 161

X

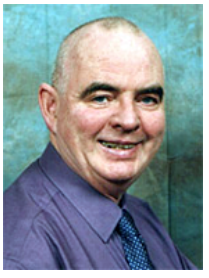
Xbootmgr.exe 723
XML Paper Specification (XPS) 367
XOR (Exclusive OR) 333
Xperf.exe 722
Xperfview.exe 722

Z

Zeitplan konfigurieren 227
Zeitzonen 132
Zero Touch Installation (ZTI) 72, 145
Zertifikate
Anmeldeinformationsverwaltung 493
Certificate of Authenticity (COA) 81
Datenwiederherstellungsagenten (DRAs) 559
DirectAccess 520
EFS und Heimnetzgruppen 452
Fehler 636
Internet Explorer, Zertifikatsperrprüfungen 627
Smartcards 498f.
SSL-Zertifikate konfigurieren 634–637
Verschlüsselndes Dateisystem (EFS) 450
Verwalten 502ff.
VPN-Authentifizierungsprotokolle 533f.
Wiederherstellungsagenten 451f.
Zertifikatregeln 270, 274
Zertifikatspeicher, Gerätetreiber 212–215
Zertifikate anzeigen 634
Zertifikate-Konsole (Certmgr.msc) 502ff.
Zertifizierungsstelle
Benutzerkontensteuerung (UAC) 484, 486
DirectAccess 520
Drahtlosadapter, Sicherheit 356ff.
Gerätetreiber 212–215
SSL-Zertifikate konfigurieren 634
Windows-Firewall mit erweiterter Sicherheit (WFAS) 391
Zielpfad 134f.
Zonen-ID 339
Zonenregeln 270
Zugriffssteuerungslisten (ACL) 39
Zulassen 315
Zuverlässigkeitsüberwachung 210, 661f.

Zwischenspeichern
BranchCache
Konfigurieren von Clients 461–466
Modus Gehosteter Cache 460
Modus Verteilter Cache 460f.
Übersicht 459f.
Übung, BranchCache-Konfiguration 468f.
Windows Server 2008 466f.
Zwischenspeichern *(Fortsetzung)*
Nachbarcache 339
Negative 312
Offlinedateien 574–582
Offlineeinstellungen 428
Optionen für freigegebene Ordner 430
Schreibcache konfigurieren 715f.
Transparente Zwischenspeicherung 577f.

Die Autoren



Ian McLean, MCSE, MCITP, MCT, kann über 40 Jahre Erfahrung in Industrie, Handel und Ausbildung vorweisen. Er begann seine Karriere als Elektronikingenieur, bevor er im Bereich Fernstudium tätig war und dann Universitätsprofessor wurde. Derzeit betreibt er seine eigene Beratungsfirma. Ian hat über 20 Bücher und viele technische Artikel geschrieben. Mit Microsoft-Betriebssystemen arbeitet er seit 1997.



Orin Thomas ist Autor und MCT. Er hat über ein Dutzend Trainingsbücher für Microsoft Press geschrieben. Er hat mehrere Zertifizierungen, unter anderem als MCSE und MCITP. Er ist Vorsitzender der Melbourne Security and Infrastructure Interchange und ein Microsoft-Sicherheits-MVP. Er lebt mit seiner Frau und seinem Sohn in Melbourne, Australien, und genießt es, um die Welt zu reisen und auf Technikkonferenzen wie Tech.ED Vorträge zu halten.